PATENT ABSTRACTS OF JAPAN

(11)Publication number : **2002-175505**

(43)Date of publication of application : **21.06.2002**

(51)Int.Cl. G06K 17/00

G06K 19/10

H04L 9/32

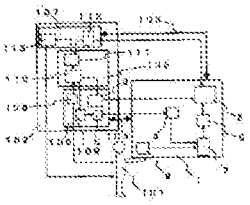
(21)Application number : **2000-374056**

(22)Date of filing : **08.12.2000**

(71)Applicant : **CITIZEN WATCH CO LTD**

(72)Inventor : **KOSAKA AKINORI**

(54) **PORTABLE INFORMATION DEVICE, PERSONAL IDENTIFICATION SYSTEM, AND IDENTIFICATION DATA ERASING METHOD**



(57)Abstract:

PROBLEM TO BE SOLVED: To solve the problem that the danger of a decrease in convenience due to the complexity of a managing means, a deficiency in the storage capacity of an information device and a leak of identification information expands since plural pieces of identification data are stored in one personal portable information device as use fields of an individual

identification system are diversified.
SOLUTION: This system is provided with a means which stores conditions of the erasure of identification data as condition data and a means which optionally erases the identification data by using the condition data.

* NOTICES *

CLAIMS

[Claim(s)]
[Claim 1]An authentication data input means which inputs authentication data from the outside in a portable information device used for personal authentication, An authentication data memory measure which memorizes said authentication data, and a condition data input means which inputs condition data which sets up conditions for eliminating said authentication data from the exterior or an inside, A condition data memory measure which memorizes said condition data, and a control data input means which inputs control data from the exterior or an inside, A portable information device having a processing judging means which processes and judges said control data and said condition data, and an authentication data erasing means which eliminates said authentication data, and eliminating said authentication data based on a decision result of said processing judging means.
[Claim 2]The portable information device according to claim 1 providing said

control data input means with the communications department which receives electromagnetic waves from the outside, and receiving said control data by electromagnetic waves from the outside.

[Claim 3]The portable information device according to claim 1 providing said control data input means with an input part which inputs data with an input button or an input interface, and inputting said control data from said input part.

[Claim 4]The portable information device according to claim 1 providing said control data input means with a hour entry receive section which acquires a hour entry from a hour entry generating part which acquires a hour entry, or the exterior, and obtaining said control data from said hour entry.

[Claim 5]The portable information device according to claim 1 providing said control data input means with a biological information sampling section which acquires biological information, and obtaining said control data from said biological information of a user.

[Claim 6]The portable information device according to claim 1 providing said control data input means with a position information acquisition part which acquires position information, and obtaining said control data from said position information.

[Claim 7]The portable information device according to claim 1 providing said control data input means with a signal output part having a sensor, and obtaining said control data from a signal generated in said signal output part.

[Claim 8]The portable information device according to claim 1 providing said control data input means with a signal output part by power generation means to build in or a charging means to build in, and obtaining said control data from a signal generated in said signal output part.

[Claim 9]The portable information device according to claim 1 eliminating said authentication data because condition data which said processing judging means has a condition data alteration means which changes said condition data with said control data, and was changed by the input of said control data fulfills the appointed conditions.

[Claim 10]The portable information device according to claim 1, wherein said

authentication data memory measures are some data required for authentication data to memorize to carry out personal authentication.

[Claim 11]The portable information device according to claim 1, wherein said authentication data memory measure memorizes two or more authentication data.

[Claim 12]The portable information device according to claim 1, wherein said condition data memory measure memorizes one condition data for eliminating two or more authentication data.

[Claim 13]The portable information device according to claim 1, wherein said condition data memory measure memorizes two or more condition data for eliminating one authentication data.

[Claim 14]The portable information device according to claim 1 provided with an authentication data erasure condition reporting means which eliminates said authentication data on what kind of conditions, or is told to a user.

[Claim 15]The portable information device according to claim 1 provided with a personal authentication possible service reporting means which carries out personal authentication with authentication data which is carrying out actual condition memory, and tells available service to a user by sound or display.

[Claim 16]The portable information device according to claim 1 provided with an authentication data elimination notice means which announces eliminating said authentication data beforehand to a user.

[Claim 17]The portable information device according to claim 1 provided with an identification number memory measure which memorizes an identification number.

[Claim 18]The portable information device according to claim 1 provided with at least one of a telephone network connecting means and the Internet network connecting means.

[Claim 19]The portable information device according to claim 1 eliminating said authentication data erasing means using an external electromagnetic field or external electromagnetic waves.

[Claim 20]The portable information device according to claim 1 provided with a

condition data setting-out means to set up said condition data for memorizing to said condition data memory measure.

[Claim 21]An user specifying means which specifies a user, and an authentication data issuing means which publishes identifiable authentication data later, An authentication data input means which inputs said authentication data into the portable information device according to claim 20 from Claim 1, An authentication data reference means which refers to authentication data memorized to said portable information device, A personal identification device provided with an authentication data identification device which identifies said authentication data, and a service use permission means to which service use is permitted, It has a cable of said portable information device and said personal identification device, radio, or an information transmission line by contact, A personal authentication system inputting said authentication data into said portable information device which a user whom said personal identification device specified specifies, performing a user's personal authentication because the account personal identification device of back to front identifies said authentication data with reference to said authentication data, and permitting use of service.

[Claim 22]A condition data setting-out means by which said personal identification device sets up condition data, It has a condition data input means which inputs condition data into said portable information device, Based on a result of having processed and judged control data inputted after it inputs into said portable information device condition data set up in said personal identification device and said portable information device memorizes condition data, and said condition data within said portable information device, The personal authentication system according to claim 21 eliminating said authentication data.

[Claim 23]A user specific part in which said personal identification device has an user specifying means and an authentication data input means at least, An information processing section which has an authentication data identification device at least, and an authentication data reference part which has an

authentication data reference means at least, Have an information transmission line of a cable of a user specific part, an information processing section, and an authentication data reference part, or radio, and an authentication data reference part, Have a cable with a portable information device, radio, or an information transmission line by contact, and said user specific part, It has said portable information device, a cable and radio, or an information transmission line by contact, When said authentication data is inputted into said portable information device which a user whom a user specific part specified specifies, and said information processing section identifies said authentication data after an authentication data reference part refers to said authentication data, The personal authentication system according to claim 21 permitting a user's service use.

[Claim 24]The personal authentication system according to claim 23, wherein said user specific part is provided with a condition data setting-out means and a condition data input means.

[Claim 25]In an authentication data erasing method used with a portable information device for personal authentication, An authentication data erasing method which eliminates said authentication data when said portable information device identifies a signal which inputs and memorizes conditions corresponding to authentication data and said authentication data from Claim 1 to a portable information device given in any 1 paragraph of Claim 20, and with which it is satisfied of said conditions.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not

reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the portable information device used with the personal authentication system used for an introduction, a ticket gate, logon to a computer, credit processing, a cash advance, article transaction, and service of rental equipment use etc.

It is related with the portable information device, personal authentication system, and authentication data erasing method for the personal authentication which realizes improving the safety of a personal authentication system, and efficiency especially for the system donor and user of a personal authentication system.

[0002]

[Description of the Prior Art]When a personal authentication system uses service, it is a security system which checks that he is the permitted just user. It is referred to as carrying out personal authentication to attest a user with the information processing system which manages service of an introduction, a ticket gate, logon in KOMPYUTA, credit processing, a cash advance, article transaction, rental equipment use, etc. A user's attestation is attestation of the user who checks that he is the just user permitted to the Data Processing Division handbook (volume for 1st 1989 edition Information Processing Society of Japan) among the external security of a description, internal SEKIRYUTI, and a user's attestation as security countermeasures of an information processing system. the utilizing method which has spread most is that the device which manages a system refers to what only the person himself/herself has in the

cases, such as login to an introduction, merchandise purchase, and a computer, -- a user -- a user -- it presumes that he is the person himself/herself and it becomes possible to receive service. Now, a password and the method of using a credit card are common. However, there is a problem in safety that there are few means to specify that these personal identification methods are original users, and they are easy to be used by others. However, the service using a personal authentication system has spread in society from the convenience, and the safety of the personal authentication system is further asked in Electronic Commerce Technology Division using the Internet.

[0003]The personal identification method which transposes a password etc. to complicated data and uses them using an IC card with a recent years comparatively big storage capacity is ****** at the beginning of spread. For example, the personal authentication system high [the safety which processes data including the biological information of the individual who memorizes in a card, and the biological information actually acquired at the spot to attest, judges whether it is in agreement and carries out personal authentication], and flexible is devised. If the data needed for personal authentication is called authentication data, it will judge with the authentication method using an IC card being that authentication data including a lot of personal information is memorized by the storage of one sheet, and being a just user. It is the comparatively simple method that safety and reliability are high, under the premise of using the living body feature which only an individual cannot have. The utilizing method which makes these memorize authentication data and carries out personal authentication in a place where one has gone by the spread of portable information devices, such as a cellular phone linked to the Internet, is also considered. A user's convenience improves because a user uses the portable information device carried every day with two or more personal authentication systems, and two or more cards are possessed or it is released from inconvenient [which memorizes two or more passwords on the head]. The side which provides a system also becomes possible [calculating increase in efficiency about the system which two or more users use] by

carrying out personal authentication of two or more portable information devices quickly by data communications. However, a possibility of there being a danger of flowing out a lot of [detailed and] personal information and the information on the bodily features of the individual who cannot be changed by loss of a portable information device, simultaneously with the spread using a portable information device of personal authentication systems, and producing SUBJECT at safety is also high. In order to carry out personal authentication by data, while updating old authentication data frequently to new authentication data and securing safety, management of efficient authentication data is also needed.

[0004]In an IC card, a portable information device, etc., the method of eliminating authentication data, or making it unusable and securing safety is devised, and it is [put in and]. Authentication data is data used for identifying and carrying out personal authentication of the user to whom use was permitted, those to whom use is not permitted, or other users with a personal authentication system, and it has a means to identify after issue. . For example, the internal security control of copy protection, such as encryption, or the prevention from an illegal use should do. possessing these including password information, the information by action of a signature etc., biological information, including biometrics etc., the information read in the storage, and article transaction certification information -- a user -- the person himself/herself is identified. What is necessary is just to use an electronic key, a part of an electronic key, etc. which use encoding technology, for example with a means to identify after issue. Discernment of authentication data of the device which carries the portable information device with which the user memorized authentication data beforehand to the spot which receives service and with which a system donor manages it as a utilizing method will permit a user use of service. A system donor is the person and organization which provide service to a user using a personal authentication system. Since it is data, more than one can be memorized to one portable information device, or it can eliminate with sufficient convenience, or can update to a new thing. The quick attestation at

the spot with many users of the system which carries out personal authentication only by referring to authentication data is attained.

[0005]The unauthorized use arrester (Japanese Patent Application No. 8-274136) of an IC card, When it has a receive section which receives a radio signal to an IC card, and a storage parts store which memorizes the data for identifying an owner and the predetermined time reception of the predetermined radio signal cannot be carried out in a receive section, the authentication data memorized to the storage parts store is made into elimination or a use impossibility. When an IC card is lost or a theft is encountered by this, it cannot be used promptly and carries out. If the information device and input device (Japanese Patent Application No. 11-282981) of a personal authentication system have a means to detect a body wearing state to a portable information device and secession of the portable information device from a user is detected, they will make unusable the authentication data stored in the portable information device. The improvement in convenience -- although these are considered about safety, authentication data is simply eliminated by the composition with which an IC card and a portable information device are equipped, and they eliminate arbitrarily authentication data with specific user and system donor -- is difficult. Improving safety to each in the memorized authentication data is not indicated, but correspondence is difficult for efficient management of authentication data, effective use of the storage capacity of a portable information device, and diversification of the field of the invention of a personal authentication system.

[0006]

[Problem(s) to be Solved by the Invention]As mentioned above, it is possible that the field of the invention of a personal authentication system sets to be diversified, and a new problem arises at efficiency and safety. Two or more authentication data is especially memorized to one portable information device which an individual owns, SUBJECT is produced from danger expansion of shortage of the storage capacity of a portable information device, or the information leak for attestation at the efficiency of a system, and safety because

the fall of the convenience by complication of the management tool of the data used for attestation using at two or more service spots and authentication data unnecessary after use remain.

[0007]This invention was made in view of said problem, and an object of this invention is to provide the portable information device with which a purveyor of service and a user improve the efficiency of a personal authentication system, and safety separately especially. This application has a new function and sets it as other purposes to provide the portable information device, personal authentication system, and authentication data erasing method which improve safety and efficiency.

[0008]

[Means for Solving the Problem]An authentication data input means which inputs authentication data from the outside in a portable information device used for personal authentication, An authentication data memory measure which memorizes authentication data, and a condition data input means which inputs condition data which sets up conditions for eliminating authentication data from the exterior or an inside, A condition data memory measure which memorizes condition data, and a control data input means which inputs control data from the exterior or an inside, It has a processing judging means which processes and judges control data and condition data, and an authentication data erasing means which eliminates authentication data, and authentication data is eliminated based on a decision result of a processing judging means.

[0009]In a system donor and a user setting up arbitrarily conditions which eliminate authentication data, and inputting beforehand, when a portable information device is provided with such composition. By eliminating specific authentication data from two or more authentication data memorized when conditions are satisfied, controllability is added to each authentication data, an unnecessary outflow is prevented and safety is secured by individual management being attained. It becomes possible by stopping troubling to storage capacity reservation of a portable information device, and management of authentication data, and improving convenience to secure efficiency.

[0010]

[Embodiment of the Invention](Working example 1) Drawing 1 is a figure showing the system configuration of this invention. The portable information device with which the user memorized authentication data beforehand is carried to the spot which receives service, and a user will be permitted use of service if the device which a system donor manages identifies authentication data. It is possible that a new problem arises at the efficiency of a personal authentication system, and safety that the field of the invention of such a personal authentication system sets to be diversified, and shares and uses one portable information device. That is, in the case where two or more authentication data is memorized and used for one portable information device, The user can consider the fall of efficiency, such as troubling to storage capacity reservation of a portable information device, and management of authentication data, and also the safety that the outflow frequency of the authentication data which included personal information according to the theft of the portable information device, etc. increases has SUBJECT.

[0011]In a system donor and a user setting up arbitrarily the conditions which eliminate authentication data, and inputting into a portable information device beforehand in this invention. When conditions are satisfied, specific authentication data is eliminated from two or more authentication data memorized in a portable information device, controllability is added to each authentication data, and individual management is attained. The unnecessary information leak made by this since the authentication data after using it at the time of a theft was memorized in the portable information device is prevented. By what is automatically eliminated after use although complicate authentication data greatly, and safety is improved or two or more authentication data is used according to the purpose. The storage capacity of a portable information device is secured efficiently, it is lost that a user receives the troublesomeness of management in using further two or more authentication data, and it becomes possible to update and use for authentication data new further always. Correspond to diversification of the field of the invention of a personal

authentication system, such as using one portable information device with two or more personal authentication systems, or carrying out personal authentication only by communication of data, and for a user and a system administrator Thus, safety, The portable information device excellent in efficiency, a personal authentication system, and an authentication data erasing method are provided.

[0012]Drawing 1 consists of the information transmission lines 103 and 104 of the portable information device 1, the personal identification device 102, the user 101, and the portable information device 1 and the personal identification device 102. The personal identification device 102 has the user specific part 105, the information processing section 106, and the authentication data reference part 107, the user specific part 105 communicates by the portable information device 1 and the information transmission line 104, and the user reference part 113 communicates by the portable information device 1 and the information transmission line 103. By making the personal identification device 102 such composition, the user specific part 105 and the information processing section 106 are installed inside a domestic door, only the authentication data reference part 107 is installed in the outside of a door, and it corresponds to diversification of a system, such as securing the safety of a personal authentication system. The user specific part 105, the information processing section 106, and the authentication data reference part 107 may be separated, two or more sets may be installed, each may be connected by an information transmission line, and it may use as one device. 1 of drawing 1 is a portable information device, and an individual carries it -- as -- a weight saving -- the power is saved. Mainly A cellular phone, PHS, a portable computer, a wrist watch, and wristwatch type information machines and equipment, It is a portable information end, a handheld game machine, portable equipment that inserts an IC card and functions, and the apparatus which composite-ized these apparatus, and personal authentication is carried out at the spot which receives service because the portable information device 1 has memorized authentication data, and the user 101 is permitted receiving service. 2 is an

authentication data memory measure and memorizes authentication data. Memory storage thinks as important a semiconductor device, a magnetic drive, and memorizing authentication data safely, although there are an optical disc etc. in some numbers, and should just choose them in consideration of the airtightness of a personal authentication system by the power-saving nature of the portable information device 1, lightweight nature, endurance, and cost. It is good also as a storage for distribution to insert storages, such as an easy IC card, in the portable information device 1 like a cassette or a card. It memorizes with memory storage using electrical and electric equipment, magnetism, light, etc. 3 is an authentication data input means and is inputted from the portable information device 1 outside.

[0013]In drawing 1, it inputs into the portable information device 1 according to the information transmission line 104 from the user specific part 105. In order to make the portable information device 1 correspond with the user 101 with authentication data, it is necessary to input into the specific portable information device 1 specified by the user 101 who specified. The specific method of the portable information device 1 by the peculiar identification number which referred to the specific method of the portable information device 1 at the time of the user's 101 specification, There are a method of inputting into the portable information device 1 which is communicating by the user specific part 109 and the information transmission line 104 at the time of the user's 101 specification, the method of inputting into the specific portable information device 1 which connects with the user specific part 109 in user 101 specification, and is not checking secession, etc.

[0014]4 is a condition data memory measure, and in order to use for eliminating specific authentication data, it memorizes condition data in the portable information device 1. Although it may memorize by the same method as authentication data and memory storage may be the same, read-out is freely possible for processing condition data. Condition data is data which can be processed, and if conditions are satisfied including the conditions which eliminate corresponding specific authentication data at least, the specific

authentication data in the portable information device 1 will be eliminated. In order to eliminate authentication data within the portable information device 1, a program including the authentication data procedure which eliminates authentication data specific besides conditions, and the condition data procedure which processes and judges whether conditions were fulfilled or not may be included in condition data. In addition, since the specific control data inputted arbitrarily [in order that condition data may eliminate authentication data], and the control data procedure to process may be added or condition data may be eliminated simultaneously with authentication data, the procedure which eliminates condition data after use may be included in condition data procedure. Programs included in condition data, such as conditions and a procedure, need to set up the contents in accordance with the kind of control data inputted by the control data input means 8 of the portable information device 1, or the control data input means 707 from the outside. For example, control data procedure is automatically added so that the control data input means 8 and 707 which the portable information device 1 or the personal identification device 701 has may be checked and specific control data may be processed, before and after inputting and memorizing authentication data, Furthermore, the user 101 etc. set up and add suitable conditions to control data. In addition, the authentication data which is not freely eliminable may be eliminated by using authentication data procedure. 5 is a condition data input means and is inputted from the portable information device 1 outside. Condition data may be inputted by portable information device 1 inside.

[0015]In drawing 1, it inputs into simultaneous with authentication data, or order according to the information transmission line 104 from the user specific part 105 which is the exterior. 6 is an authentication data erasing means and eliminates the authentication data memorized by the authentication data memory measure 2 after the judgment which eliminates the authentication data based on the processing judging means 7. A thing eliminable with a memory storage simple substance like a semiconductor device or a magnetic drive has all elimination mechanisms in portable information device 1 inside. In order to

eliminate using an external electromagnetic field or external electromagnetic waves, only the exterior of the portable information device 1 is eliminated combining the composition of the exterior and an inside. For example, an erasing method like the magnetic card which eliminates authentication data by holding up the portable information device 1 to the electromagnetic field which the personal identification device 102 emits, and the erasing method which eliminates authentication data by irradiating the portable information device 1 with ultraviolet rays may be used. Elimination is erasing information or overwriting for other information so that it cannot read, even if it uses authentication data every means from the portable information device 1, and in working example. by elimination, personal authentication becomes impossible, that is, it is ****** not only about the user 101 but about the portable information device 1 -- for an offender, service use is not permitted. After satisfying condition data, by eliminating automatically, the storage capacity of the portable information device 1 can be secured efficiently, or the user 101 can also save the time and effort eliminated after service use.

[0016]7 is a processing judging means, and processes and judges condition data and control data. Processings are a series of work done to data, in order to acquire required information. For example, read data, create data, eliminate data, or. It is it having been in agreement as a result of amended data, or data's identified other data, or having compared compared data with other data, or computing the variation of data, an error amount, constant value, and average value before comparing or comparing, or comparing or comparing, or obtaining the result of no. The required information in the processing judging means 7 is information on whether authentication data is eliminated. It judges having acquired the information on whether authentication data is eliminated by not filling, or it processes the condition data previously remembered to be the inputted control data and control data mainly fulfills conditions especially by this example. 8 is a control data input means, and control data is data used as the cause which eliminates authentication data, and it may include in condition data by making the procedure to fix into control data procedure etc. Especially in this

example, specific authentication data is eliminated by using as control data the data with which it is satisfied of the conditions of condition data, inputting it into the portable information device 1, and processing it with condition data. Only when required, it may input, may input without an interval, or may input intermittently, and what is necessary is just to choose by the kind of authentication data, or composition of the portable information device 1. For example, what is necessary is to input the control data received by electromagnetic waves, only when it receives, and the control data based on biological information needs an intermittent input, in order to know whether the variation of the control data which is the data which sampled the user's 101 biological information periodically will fulfill conditions. At drawing 1, it inputs by portable information device 1 inside. Control data has two or more kinds as it is shown in drawing 5.

[0017]It is a personal identification device, and 102 inputs authentication data into the specific portable information device 1 of the user 101 who specified, is the service spot behind, is identifying with reference to the authentication data memorized to the portable information device 1, and is a device which carries out personal authentication. The user specifying means 108 which specifies the user 101 at this time, and the authentication data issuing means 110 which publishes identifiable authentication data later, It has the authentication data input means 3, the authentication data reference means 112 which refers to the authentication data memorized to the portable information device 1, just authentication data or the authentication data identification device 111 to identify, and the service use permission means 113 to which service use is permitted. Those whom the personal identification device 102 has, in addition to this, permitted neither a user nor use with the user 101 by having these means using the portable information device 1 are identified at the service spot.

[0018]105 is a user specific part and has the user specifying means 108 and the authentication data input means 3 at least, In addition, if it has the condition data input means 5 and the condition data setting-out means 109, while the user 101 will look at a screen on that spot, it is beforehand [, such as choosing

conditions,] ready for eliminating authentication data automatically, and convenience improves. It checks that the user 101 using authentication data can specify that he is the just user permitted to the system donor, for example, the user specifying means 108 can be collected. By beginning a user's specification, the authentication data used for behind with the user 101 is made to correspond, and use of a personal authentication system is started. knowing the password as the user's 101 specific method -- or, the identification number of the portable information device 1 to own -- or, The method of using a password and specifying a user, and besides it, a computer, The user specific part 105 is installed in the large-sized end of a convenience store, etc., How to measure biological information, including biometrics etc., and compare with the past measurement data etc., The method that various reliability is high is used, or a method and all with convenience should just choose specification by storages, such as a creditor card and an IC card, the specification as a person which only purchased goods and a use right, etc. with required efficiency and reliability. Automatic, or the user 101 and a system donor sets up authentication data procedure, condition data procedure, control data procedure, etc. by a procedure out of the conditions which need to set up the condition data setting-out means 109 at least. For example, control data procedure is automatically set up by the kind of control data input means 8 which the portable information device 1 has, and conditions are set up because the user 101 chooses from two or more conditions which the system donor set up beforehand from the panel on the user specific part 301.

[0019]106 is an information processing section, had the authentication data identification device 111 at least, and may put in a database and manage personal information, such as Assessment on Search Report by Designated Searching Authority, by computer etc. At this time, the authentication data issuing means 110, and authentication data and the data for authentication data discernment which were had and published may be managed in a unified manner within a database. The user's 101 specification and specification of the portable information device 1 come out surely, and, in between [a certain], the

authentication data issuing means 110 publishes identifiable authentication data later. The identifying method of the authentication data based on the authentication data identification device 111, A part required to carry out personal authentication like an electronic key by the authentication data issuing means 110 is inputted into the portable information device 101 as authentication data, The data for authentication data discernment which is other parts is published simultaneously, and when carrying out personal authentication, the authentication data referred to with the portable information device 1 may be used by the authentication data identification device 111. Include the information for specifying the user 101 in the authentication data issuing means 110 as the other methods, and the identification number of the portable information device 1 in authentication data, and they are published, What is necessary is for there to be the method of performing specification of the user 101 or the portable information device 1 again at the time of personal authentication, and using by the authentication data identification device 111, etc., and just to use the issuing method of the authentication data which was suitable by composition of the system, etc.

[0020]107 may have the authentication data reference means 112 at least by an authentication data reference part, in addition may have the service use permission means 113. Refer to the authentication data memorized to the portable information device 1 for the authentication data reference means 112 using the information transmission line 103. Reference is work of a series performed for accumulating which acquires the information which identifies the authentication data memorized to the authentication data memory measure 2, and are establishment of the data-transmission-and-reception means to the authentication data memory measure 2, detection of data, the check of the existence of data, reading of data, and a series of work compared or compared. The same correspondence procedure may be sufficient as the information transmission line 103 and the information transmission line 104. The portable information device 1 has a radio cellular-phone connecting means and an Internet connectivity means, and them communicate using this or, As it

communicates by communicating using electromagnetic waves, such as short-distance-radio communication and infrared rays, connecting by a cable, or contacting in devices, the outflow of authentication data may be suppressed as much as possible. If the service use permission means 113 is discriminated from the just authentication data which published the authentication data referred to at the time of the user's 101 specification, use will be permitted for service. For example, if it is a ticket gate and an introduction, a door will open, or it indicates that it is the person himself/herself if it is delivery of goods, or logon of a computer is made, and service is received. Thus, unlocking of a door, opening and closing, the ticket gate of a vehicle, the operation start of a computer, the individual signature input by a computer, the contract sending by a computer, and a user -- it is based on fields of the invention, such as the proof display of being the person himself/herself, balancing account of merchandise purchase, a deposit of cash, payment of cash, refundment of cash, and an operation start of apparatus.

[0021]Correspondence of the authentication data and condition data which memorize drawing 2 to a portable information device, the lineblock diagram of the personal authentication system with which drawing 3 contained a portable information device and this, The lineblock diagram of the personal authentication system with which drawing 4 contained a portable information device and this, the figure showing the relation of the composition which needs drawing 5 for a control data kind and a control data input means, The lineblock diagram of the personal authentication system which drawing 6 showed the details of the portable information device, and drawing 7 are the lineblock diagrams of the personal authentication system with which drawing 3 contained a portable information device and this.

[0022]Drawing 2 shows correspondence of the authentication data and condition data which are memorized to the portable information device 1. The user 101 uses two or more personal authentication systems because the portable information device 1 memorizes two or more authentication data. Authentication data A is personal authentication system A, authentication data

B is personal authentication system B, and authentication data C is used for personal authentication by personal authentication system C. When authentication data A and authentication data D are arranged, the utilizing method which carries out personal authentication by personal authentication system D is also good. Personal authentication system A to D is provided with the respectively original personal identification device, and a separate system donor may manage it. Although the sizes of authentication data differ in a figure, the size of authentication data is expressed. although the data in which internal security was fully made generally becomes large, large authentication data is used with all the personal authentication systems -- it does not need and a purveyor of service should just choose if needed. The size also changes with the conditions and procedures also containing condition data.

[0023]Condition data A is memorized in order to eliminate authentication data A, and if the conditions of condition data A are satisfied, it will eliminate only authentication data A from the portable information device 1. If authentication data B satisfies the conditions of condition data B, it will be eliminated, but it is eliminated even if it satisfies the conditions of condition data C. Satisfaction of the conditions of condition data C will also eliminate authentication data C with authentication data B. The condition data in which authentication data D corresponds in order that the user 101 may set up condition data on the portable information device 1 after an authentication data input does not exist. In unimportant authentication data, condition data may be set up as usual and you may also drop off. Condition data D is condition data already inputted at the time of shipment of the portable information device 1, and the user 101 sets up eliminate the specific authentication data memorized on the portable information device 1. Operativity improves by preparing condition data a priori together with the kind of control data input means 8 with which the portable information device 1 is provided.

[0024]Drawing 3 is a lineblock diagram of the personal authentication system which the system donor from whom the personal authentication system of drawing 1 differs provides. The portable information device 1 which the user

101 uses is the same. The means which it has although the personal identification device 102 and the different personal identification device 301 are used in this personal authentication system is the same as that of the personal identification device 102. Differing is a point which separates the user specific part 304, the information processing section 305, and the authentication data reference part 306, and is installed in somewhere else. Although owners may differ, and personal authentication is carried out, they operate as one device, respectively. The user specific part 304, the information processing section 305, and the authentication data reference part 306 are connected by the information transmission lines 302 and 303, respectively. For example, it becomes easy to respond to diversification of a system by arranging the user specific part 304 at a home, arranging the authentication data reference part 306 to the retail store of the service spot, etc., and arranging the information processing section 305 in a system donor's company. Two or more user specific parts 304 and authentication data reference parts 306 may exist, and are managed in a unified manner by at least one information processing section 305. The user specific part 304 has the user specifying means 311 and the authentication data input means 309, the information processing section 305 has the authentication data identification device 312, and the authentication data reference part 306 at least has the authentication data reference means 313 at least. In drawing 3, the user specific part 304 has the condition inputting means 310 further, and the authentication data reference part 306 has the control data input means 314 further. What is necessary is just to choose the condition data setting-out means 109 which the personal identification device 102 of drawing 1 has, the authentication data issuing means 110, and the service use permission means 113 etc. and the same means with the operation method of the information transmission line which may be built in anywhere in the personal identification device 301, and is used, or a system. However, the personal identification device 306 needs to be a device authorized on the level which a system donor manages enough, and which was device [the level] or wished to have. For example, if there is no reliability of 306 user specific part installed in a home for

a system donor, the reliability of authentication data will also be lost.
[0025]Drawing 4 is a detail view of a portable information device. In drawing 4, the portable information device 1 of the user 101 who specified is specified from two or more portable information devices using the identification number memorized to the identification number memory measure 407 of the portable information device 1, and authentication data is inputted. An identification number is a number which can specify the portable information device 1 by this, and if it applies to a telephone number or this if had, and the portable information device 1 has [a wire telephone connecting means, a wireless telephone connecting means, or] an Internet connectivity means, it will apply to an address number or this. It becomes possible to also perform collection of money to a system donor efficiently by using a reliable identification number.
[0026]The condition data input means 402 is the method of inputting condition data by portable information device 1 inside as other input methods of the method of inputting from the personal identification device 102 which is the portable information device 1 exterior like the condition data input means 5. Simultaneously, the portable information device 1 specifies the authentication data which has the condition data setting-out means 406, and eliminates it from two or more memorized authentication data, and eliminates it on what kind of conditions, or the user 101 sets it up automatically. A program including authentication data procedure and condition data procedure other than conditions, control data procedure, and a condition data elimination procedure are added. It is necessary to set up condition data according to the control data input means 8 with which especially the portable information device 1 is provided. After setting up some conditions, condition data procedure, and control data procedure at the time of shipment of the portable information device 1 and memorizing authentication data, the method of setting up authentication data procedure and inputting as condition data is also.
[0027]Besides it, the portable information device 1 may have a means to notify the user 101 of the following thing. The authentication data erasure condition reporting means 403 which reports on what kind of conditions the authentication

data to memorize is eliminated, The authentication data elimination notice means 405 etc. which the authentication data to memorize makes the personal authentication possible service reporting means 404 which reports whether personal authentication is possible, and the advance notice from which authentication data is eliminated with which personal authentication system. The user's 101 convenience in the personal authentication system which used the portable information device because the portable information device 1 has these means improves.

[0028]Drawing 5 shows composition required for a control data kind and a control data input means. A control data input means inputs control data from the indicated composition. An input means has the control data input means 707 from the portable information device 1 outside like drawing 1 like the control data input means 8 in the portable information device 1, and drawing 7. The kind of control data has the control data obtained from the electromagnetic waves received from the outside, control data inputted from an input part, control data obtained from a hour entry, control data obtained by biological information, and control data obtained by signaling information. It explains below, respectively.

[0029]The control data obtained from the electromagnetic waves received from the outside uses a radio telephone network, the short distance communication method, etc., and inputs them using electromagnetic waves. It will input from the portable information device 1 outside, or will input from the communications department with which the portable information device 1 is equipped. For example, a system donor becomes possible [eliminating authentication data arbitrarily in communication available area]. If authentication data A is eliminated by receiving control data A, the system donor will input condition data A corresponding to control data A and authentication data A to process a priori from the personal identification device 102. It uses for the user 101 and a system donor inputting the control data inputted from an input part, and eliminating it from the input button with which the portable information device 1 is equipped, and an input interface arbitrarily. In the input from the hour entry

generating part with which the portable information device 1 is equipped, the control data obtained by a hour entry is arbitrarily eliminated by the date and time. In the input from the biological information sampling section with which the portable information device 1 is equipped, the user 101 detects death, poor health, etc. and the control data obtained by biological information eliminates. The control data obtained by position information will be eliminated if a certain position is exceeded by vast position information in the input from the position information acquisition part with which the portable information device 1 is equipped. The control data obtained by signaling information will be eliminated, if other human beings contact and desorb an information device and detect poor health in the input from the sensor part with which the portable information device 1 is equipped. For example, the thermo sensor and pressure sensor in which the situation where the portable information device 1 set is shown, A humidity sensor, an air pressure sensor, photosensor, and a pressure sensor, It is a various sensor which measures the living body parameter measurement mechanism relevant to an image sensor, a biosensor, a magnetic sensor, the body temperature of the users 101, such as distance sensors, a living body pulse, a pulse, humor constituents, a blood flow, etc., the current value generated by body temperature etc., and a pressure value. It has a means by which the portable information device 1 measures a situation directly, and safety is improved by setting up the conditions which eliminate authentication data arbitrarily with condition data by the authentication data escape prevention adapted to the user 101 in the attestation spot, or the situation of the portable information device 1.

[0030]In working example, the portable information device 1 has a hour entry generating part as the authentication data input means 8, has the control data input means 8 which inputs control data by a hour entry, and also the communications department, and inputs control data into the portable information device 1 by the control data input means 707 from the personal identification device 102.

[0031]Drawing 6 shows the lineblock diagram of an authentication data erasing

method. It is the composition which changes condition data and eliminates authentication data eventually. The portable information device 1 changes condition data by what is necessary's being just to have the condition data alteration means 601, and inputting control data by an input part as the control data input means 8. Out of it, condition data inputs control data for every service use by the control data input means 8 including the information on the service use limit count, The portable information device 1, such as carrying out the judgment which fulfilled conditions, if said service use limit count is subtracted by the condition data alteration means 601 of the processing judging means 7 and it is set to 0, and eliminating specific authentication data by the authentication data erasing means 6, is used, A coupon ticket and use like a prepaid card are enabled.

[0032]Drawing 7 shows the lineblock diagram of the authentication data erasing method of working example 1. If it is an input of the control data from the communications department 702, it will become the same authentication data erasing system composition as drawing 1, but if the control data input means 704 presupposes that it has in the personal identification device 102 and the input origin of the control data based on electromagnetic waves is clarified, it will become like drawing 7. In working example, the authentication data erasing method using drawing 1 and the authentication data erasing method using drawing 7 are used. It consists of the portable information device 1, the personal identification device 102, the information transmission line 103, and the information transmission line 104 using the wireless telephone communications network 701. 703 may have the communications department of the personal identification device 102, 702 may have a wireless telephone connecting means and an Internet connectivity means in the communications department of an information device, and it uses for communication of a radio telephone network in working example. If the certain conditions same inside the personal identification device 102 as the portable information device 1 are fulfilled, the system which inputs control data into a portable information device will be constituted, and control data will be inputted by the control data input

means 704 of the personal identification device 102. At this time, the user's 101 portable information device 1 is specified from many portable information devices with the identification number clarified at a user's specific time. If it judges with the received electromagnetic waves being the arbitrary control data transmitted from the personal identification device 102, the conditions of condition data will be fulfilled by the portable information device 1, and authentication data will be eliminated with it. It is necessary to set a priori the control data procedure which processes the arbitrary control data of a transmitting schedule to condition data, and to add it to it. The information transmission line 103 is used by the authentication data reference means 112, and electromagnetic waves are not used, but another low safe correspondence procedure of the danger of outflows, such as contact, is used.

[0033]The flow chart of working example 1 is shown in drawing 8. In the above, working example 1 is described below using drawing 1, drawing 2, drawing 3, drawing 4, drawing 5, drawing 6, and drawing 7.

[0034]Drawing 1 is a personal authentication system used in an event site. However, like the personal identification device 301 of drawing 3, the user specific part 105, the information processing section 106, and the authentication data reference part 107 communicate according to the information transmission line which is separated and installed and connects each at the time of operation, and a system donor manages the personal identification device 102, and they own it. An entrance right with the term of validity of an event is purchased by communication with the user specific part 105 on the screen of the portable information device 1 which the user 101 owns, and authentication data B is memorized to the portable information device 1. Furthermore, communication with the authentication data reference part 107 shows authentication data B, personal authentication is carried out, and a private school is entered in an event site. Authentication data B memorized to the portable information device 1 is automatically eliminated by passing over the term of validity or receiving specific control data. A personal authentication preparatory step, a personal authentication stage, and an authentication data elimination stage are shown in

drawing 8. the input 806 of the specification 801 of the user of drawing 8 to condition data is a personal authentication preparatory step, and referring to the authentication data B is possible -- 807 to the service starts 810 are personal authentication execution phases, and the control data input 811 to the service use right lapse 814 is an authentication data elimination stage.

[0035]A personal authentication preparatory step is the entrance spot of the event site which receives service, and is a preparatory step which carries out personal authentication using the portable information device 1 with which the user 101 memorized authentication data B. The authentication data identifiable [both] at the time of personal authentication whose portable information device 1 is made to correspond with the user 101 who specified by authentication data B is published. Condition data is inputted in order to eliminate authentication data B arbitrarily furthermore. It is investigated whether a user's specification 801 may use a personal authentication system simultaneously by specifying the user 101. In working example, the user 101 operates the portable information device 1 which has a wireless telephone connecting means and an Internet connectivity means, The user 101 purchases the use right of an event site from a system donor by presentation of an identification number on the assumption that a system donor has a collection means of a fee from the user 101 who uses an identification number peculiar to the portable information devices 1, such as a telephone number and an address number. When it purchases, it is the just simple user specifying means 108 which acts as a buyer about the user 101 who is operating the portable information device 1. The issue 802 of authentication data publishes simultaneously authentication data B and the data for authentication data discernment, and the data for authentication data discernment memorizes it by personal identification device 102 inside. The input 804 of authentication data inputs authentication data B published to the portable information device 1 specified with the peculiar identification number referred to by a user's specification 801. It is shown that personal authentication of it will be carried out if the service use right generation 805 possesses the portable information device 1 with which the user 101 memorizes authentication data B.

[0036]The setting out 803 of condition data sets up the conditions and procedure of condition data. In working example, 2 kinds of condition data B and C are inputted into the portable information device 1. If the user 101 will choose the entrance term by 19:00 on September 8 and time will be 19:00 on September 8 from the selection frame which the system donor set up, condition data B which eliminates authentication data B will be set up. The conditions of condition data B are that control data B which shows 19:00 on September 8 is inputted, The authentication data procedure from which the procedure added eliminates authentication data B by the authentication data erasing means 6 according to the result of the processing judging means 7, The condition data procedure which processes condition data B by the processing judging means 7, and carries out a processing judging with control data, The control data procedure which processes control data B including the hour entry inputted from a hour entry generating part by the processing judging means 7, and the procedure in which after-elimination condition data B also eliminates authentication data B are included in condition data procedure. Although the user 101 chooses conditions in working example, a procedure checks the composition required for an authentication data input means, processing judging means, and authentication data erasing means of drawing 5 with which the portable information device 1 is equipped, and the personal identification device 102 sets it up automatically. The system of drawing 7 is used, and in order to transmit control data C from the personal identification device 102 using the information transmission line of the wireless telephone communications network 701 and to eliminate authentication data, condition data C is set up. Although the conditions of condition data C are that arbitrary control data C which the system donor decided is inputted and authentication data procedure and a condition data elimination procedure are the same contents as condition data B, Since composition required for the kind and control data input means of control data differs between condition data procedure or control data procedure like drawing 5, they serve as the contents of the exception. Condition data B and condition data C are inputted into the

portable information device 1 by the condition data input means 5, and it memorizes by the condition data memory measure 4. The user 101 may check memorized authentication data B by the personal authentication possible service reporting means 404, and may set up arbitrary condition data D by the condition data setting-out means 406 of drawing 4. Although authentication data B is not supported in drawing 4, the authentication data procedure which eliminates authentication data B is added, and is made to correspond.

[0037]A personal authentication execution phase is the event entrance spot which receives service, and is a stage which carries out the user's 101 personal authentication using authentication data. When the authentication data reference part 107 is contacted in the portable information device 1, by the authentication data reference means 112. A user's personal authentication 809 is carried out by processing data for authentication data discernment, and authentication data B published by the issue 802 of authentication data by 807 and the authentication data identification device 111 with reference to authentication data, and carrying out discernment 808 of authentication data. If personal authentication is carried out, a gate will open the user 101 by the service use permission means 113, he will be allowed an introduction, and will become the start 810 of service.

[0038]An authentication data elimination stage is a stage which eliminates authentication data B which became unnecessary for the user 101 or a system donor, after receiving service. There is also a case eliminated without receiving service. The input 811 of control data inputs control data by the control data input means 8 or the control data input means 704. If it carries out whether condition data and authentication data are processed by the processing judging means 7, and fulfill the conditions of condition data judgment 812 and conditions are fulfilled, it will become the elimination 813 of authentication data. Condition data B and condition data C explain an authentication data erasing method independently. Elimination of authentication data B using condition data B uses the composition of drawing 1. Control data B is inputted into the portable information device 1 from the hour entry generating part, control data B is

processed according to authentication data procedure in the processing judging means 7, and condition data B is processed according to condition data procedure. If the judgment which fulfills the conditions of condition data B by the data in which arbitrary time is shown being included in control data B is made, according to authentication data procedure, authentication data B will be eliminated by the authentication data erasing means 6. Elimination of authentication data B using condition data C uses the composition of drawing 7. Control data C is inputted into the portable information device 1 from the personal identification device 102 using the information transmission line 104 at a system donor's arbitrary times. In the processing judging means 7, control data C is processed according to authentication data procedure, and condition data B is processed according to condition data procedure. If the judgment which fulfills the conditions of condition data C including arbitrary data to control data B is made, according to authentication data procedure, authentication data B will be eliminated by the authentication data erasing means 6. By elimination of authentication data B, it stops being able to carry out personal authentication, and takes service use right lapse 814. It may be made to eliminate authentication data B automatically by using frequency using the composition of drawing 6. By eliminating authentication data B from the portable information device 1 automatically by passing over the term of validity which the system donor and the user 101 set up, or receiving arbitrary control data with a radio telephone network. The outflow of the unnecessary authentication data based on a theft is prevented beforehand, the troublesomeness of management is reduced, and it becomes still more possible to utilize the storage capacity of an information device effectively.

[0039](Working example 2) It consists of a personal authentication system of the house security system used for unlocking of the door of a house, and a personal authentication system of the in-company security system used for unlocking of the door of a company. Drawing 1 and drawing 3 are the personal authentication system lineblock diagrams of working example 2. Working example 2 is described below using drawing 1, drawing 2, drawing 3, drawing 4,

and drawing 5. Two authentication data is independently used with each personal authentication system. A user does not trouble authentication data A used with a corporate security system to authentication data management while being automatically eliminated after use in the company at a corporate exit and making reservation of a storage capacity. Authentication data B used with a house security system is eliminated by destructive perception of the portable information device 1, and the input of a password for which he apologized, and prevents the outflow and illegal use of authentication data by a theft.

[0040]The personal authentication system of a corporate security system uses the system configuration of drawing 3. The personal identification device 301 is separated and installed in the user specific part 304, the information processing section 305, and the authentication data reference part 306, and authentication data A is used for it. The personal authentication system of a house security system uses the system configuration of drawing 1, and authentication data B is used for it. The personal identification device 102 and the personal identification device 301 are devices which are different, respectively, and differing from working example 1 is a point which carries out personal authentication using the one portable information device 1 which the user 101 possesses with two independent personal authentication systems.

[0041]The system configuration of the personal authentication system of a corporate security system is explained based on drawing 3. It consists of the portable information device 1 of user carrying, and the personal identification device 301 currently installed in the company. The personal identification device 301 consists of the user specific part 304 installed in the front of a gate, two or more authentication data reference parts 306 installed in inside of company each door, and the information processing section 303 which identifies the published authentication data. The user specific part 304, the information processing section 305 and also the authentication data reference part 306, and the information processing section 305 are connected by the information transmission lines 302 and 303 of the cable, respectively. Both the portable information device 1, the user specific part 304, and the portable information

device 1 and the user reference part 306 have the information transmission lines 307 and 308 which adopted the same correspondence procedure by contact. The user specific part 304 has the user specifying means 304 and the authentication data input means 309 at least, in addition has the condition data input means 310. The information processing section 305 has the authentication data identification device 312 at least, may publish authentication data A simultaneously, and may manage in a unified manner and memorize the data for authentication data discernment with a user's personal information etc. using a database etc. If the authentication data reference part 306 has the authentication data reference means 313 at least and authentication data A is identified by the authentication data identification device 312, a door will open it. Only the authentication data reference part 306 installed in the door of a corporate exit among two or more authentication data reference parts 306 has the control data input means 314.

[0042]A utilizing method is explained. The user 101 makes it contact to the user specific part 304 which has installed the portable information device 101 in the front of a gate of a company, and is further specified by biometry, such as a fingerprint, by the user specifying means 311. If in agreement with an employee's biological information measured in the past memorized to the information processing section 305, identifiable authentication data A will be inputted into the portable information device 1 in contact with the user specific part 304 by the authentication data input means 309 later. The portable information device 1 memorizes authentication data A by the authentication data memory measure 4. It is carried out simultaneously on condition that control data A is inputted by communication with the user reference part 306, The authentication data procedure which eliminates authentication data A using the processing judging means 7 and the authentication data erasing means 6, The control data procedure which processes control data A, and the condition data procedure which processes condition data A and control data A are added, and it sets up automatically as condition data A, and inputs into the portable information device 1 by the condition data input means 310. The portable

information device 1 memorizes condition data A by the condition data memory measure 4. The user 101 is contacting the authentication data reference part 306 in the portable information device 1 in a company, and personal authentication is carried out and it passes because a door opens. If the authentication data reference part 306 installed in the gate of an exit is contacted at the time of leaving, control data A will be inputted by the control data input means 314. Control data A is processed by condition data A and the processing judging means 7, is fulfilling the conditions into which control data [of condition data A] A is inputted, and eliminates authentication data A memorized to the portable information device 1 by the authentication data erasing means 6. An exit door opens before and after this, and the user 101 possesses the portable information device 1 with which authentication data A was eliminated, and goes to a house. Authentication data A for companies is changed every day, and in order to update, it becomes possible to improve safety.

[0043]The composition of the personal authentication system of a house security system is explained based on drawing 1. It consists of the portable information device 1 of user carrying, the personal identification device 102 installed in a house, and the information transmission lines 103 and 104 that adopted the same correspondence procedure by contact. The personal identification device 102 is installed in the door of a house. The user specific part 103 in the personal identification device 102 has the user specifying means 108, the authentication data input means 3, the condition data setting-out means 109, and the condition data input means 5. The information processing section 106 has the authentication data issuing means 110 and the authentication data identification device 111. The user specific part 105 and the information processing section 106 are installed inside a house, and cannot be operated [from] outside a house. The condition data setting-out means 109, the condition data input means 5, and the authentication data issuing means 110 may be in whichever of the user specific part 105 or the information processing section 106. The authentication data reference part 107 has the

authentication data reference means 112 and the service use permission means 113. The authentication data reference part 107 is installed in the outside of a door, and a door is opened by identifying with reference to the authentication data in the portable information device 1 outside a house.

[0044]A utilizing method is explained. The user 101 contacts the user specific part 105 in the portable information device 1 before going out. If the personal identification device 102 is in agreement with the identification number to memorize, it will input authentication data B into the portable information device 1. The condition data setting-out means 109 sets up automatically condition data B on condition that the control data input means 8 of the portable information device 1 is checked and a destructive impact is perceived simultaneously, and inputs it by the condition data input means 5. A program including the control data procedure which processes the signal of the impact sensor with which the portable information device 1 has condition data B as control data, condition data procedure, and authentication data procedure is also added simultaneously. The user 101 sets up condition data C on condition that data other than a password is inputted into the portable information device 1 by the condition data setting-out means 406, and inputs by the condition data input means 402. A program including the control data procedure which processes the input from the input part in which the portable information device 1 has condition data C as control data, condition data procedure, and authentication data procedure is also added simultaneously. Condition data B and condition data C are memorized to the condition data memory measure 4. If condition data B or condition data C is filled, authentication data B will be eliminated as shown in drawing 2. In a company, authentication data A and condition data A are also memorized, and two or more authentication data and condition data exist in the portable information device 1. If the password which contacts the authentication data reference part 107 of the door outside in the portable information device 1 after going home, and directs a communication start is entered into the portable information device 1, With reference to authentication data B, if authentication data B is identified by the authentication

data identification device 111, a door will open the personal identification device 102 by the service use permission means 113. If the signal with which the sensor has detected a destructive impact, such as encountering the theft of the portable information device 1 and taking out a storage cell in the middle of going home, is inputted as control data, It processes with condition data B by the processing judging means 7, and authentication data B is eliminated by the authentication data erasing means 4 by the judgment which fulfills the conditions of condition data B of perceiving a destructive impact. If the password which others mistook is entered as control data, it will process with condition data C by the processing judging means 7, and authentication data B is eliminated by the authentication data erasing means 4 by judgment that the conditions of inputting DETA ** other than a password are fulfilled.

[0045]The details of the portable information device 1 are explained about drawing 4. It has the authentication data memory measure 2, the condition data memory measure 4, the authentication data erasing means 6, the processing judging means 7 that processes and judges condition data and control data, and the control data input means 8. It has a pressure sensor which detects an input button and a shock as the identification number memory measure 407 which control data is furthermore inputted by the control data input means 314 from the personal identification device 301, and is used for the security of a house, and the control data input means 8, or a displacement sensor. If it has other control data input means shown in drawing 5, it will become possible to eliminate authentication data by it becoming impossible to be unable to receive a certain electromagnetic wave, or for a certain time to come, or to measure the user's 101 biological information, and coming outside a certain area. In addition, specify the portable information device 1 and so that arbitrary authentication data may be eliminated from the authentication data which has had and memorized the condition data setting-out means 406 and the condition data input means 402 inside, as drawing 4 shows condition data, Besides it, the portable information device 1 may have the authentication data erasure condition reporting means 403, the personal authentication possible service

reporting means 404, the authentication data elimination notice means 405, etc. The user's 101 convenience improves because the portable information device 1 has these means. Thus, by authentication data A and eliminating authentication data B from the portable information device 1 individually, it is adapted for diversification of a field of the invention, the outflow of the unnecessary authentication data based on a theft is prevented beforehand, the troublesomeness of management is reduced, and it becomes still more possible to utilize the storage capacity of an information device effectively.

[0046](Working example 3) This example is a personal authentication system used for big-ticket merchandise purchase. It explains based on drawing 1, drawing 2, drawing 4, drawing 5, and drawing 6.

[0047]Drawing 1 explains the composition of a system. The personal authentication system of this example consists of the portable information device 1 of the user's 101 carrying, and the personal identification device 102. The user specific part 105 built in the computer of two or more homes where the personal identification device 102 carries out Electronic Commerce Technology Division, It consists of the authentication data reference part 107 installed in two or more retail stores, and the one or more information processing sections 106 set to the bank which is a system donor, the card issuer, etc., although it dissociates like the personal identification device 301 of drawing 3, it is connected in the information transmission line of a cable, and it functions as one device at the time of operation. It has the information transmission line 103 of the cable which data transmits and receives by connecting with the portable information device 1, and the information transmission line 104 of the radio which used infrared rays between the user specific parts 105 and the portable information device 1 at the authentication data reference part 107. The user specific part 105 belonging to the personal identification device 102 has the user specifying means 108, the authentication data input means 3, the condition data setting-out means 109, and the condition data input means 5, and inputs into the portable information device 1 the condition data set to the authentication data published after [of the user 101] specific. If the

authentication data reference part 107 has the authentication data reference means 112 and the service use permission means 113 and contacts the portable information device 1, refer to the authentication data A for it according to the information transmission line 103. The information processing section 106 has the authentication data issuing means 110 and the authentication data identification device 111, and it becomes manageable efficiently about the authentication data identification device 111 while it manages personal information, authentication data identification data, the Assessment on Search Report by Designated Searching Authority of a personal authentication system, etc. in a unified manner using a database etc. A system donor also manages issue of authentication data with a hand by the authentication data issuing means 112, and the authentication data based on the newest encoding technology is always used.

[0048]The portable information device 1 has the authentication data memory measure 2, the condition data memory measure 4, the authentication data erasing means 6, the processing judging means 7, and the control data input means 8. In order to input control data as the control data input means 8, it has a biological information sampling section which measures biological information, and a position information acquisition part which measures position information, and as shown in drawing 6, in the processing judging means 7, it has the condition data alteration means 601. It has the composition by the control data kind shown in drawing 5, and authentication data may be arbitrarily eliminated by receiving arbitrary electromagnetic waves, becoming arbitrary time, inputting other than arbitrary passwords, or perceiving the shock by arbitrary destruction. As drawing 4 shows, the portable information device 1 may have the condition data setting-out means 406, the condition data input means 402, the authentication data erasure condition reporting means 403, the personal authentication possible service reporting means 404, the authentication data elimination notice means 405, etc. inside. By having these means, convenience improves use of the personal authentication system by the portable information device 1, and efficiency improves.

[0049]A utilizing method is explained. The user 101 inserts an IC card in the computer for Electronic Commerce Technology Division at a house, and starts communication according to the information transmission line 104 between the portable information device 1 and the user specific part 105. If in agreement with the biological information memorized to an IC card by biometry, the user 101 is specified by the user specifying means 108. Authentication data B published by the authentication data issuing means 110 is inputted into the portable information device 1 which is communicating with the user specific part 105 simultaneously using the information transmission line 104. Authentication data B is memorized to the authentication data memory measure 2 of the portable information device 1. Since the IC card has memorized best biological information uniquely, it does not walk around with it at the time of going out. Condition data B which will eliminate authentication data B if fixed change is furthermore produced by the condition data setting-out means 109 in control data B containing biological information measured value, Condition data C which eliminates authentication data B by the input of control data C including position information other than the position information on the retail store which is the purchase schedule selected by computer for Electronic Commerce Technology Division is set up. Condition data B and condition data C are inputted into the portable information device 1 by the condition data input means 5 using the information transmission line 104, and it memorizes to the condition data memory measure 4. The user 101 will set up the amount of money of application limits as conditions for condition data D by the condition data setting-out means 406 in the portable information device 1, if it checks having memorized authentication data B of the purpose to the portable information device 1 by the personal authentication service reporting means 404. Condition data D is memorized by the condition data memory measure 5. Condition data D restricts the maximum transaction money amount in one authentication data which is set as the portable information device 1 which has the condition data alteration means 601 several kinds at the time of shipment, and used the portable information device 1, and is improving safety. Like

drawing 2, although condition data D does not support authentication data B, it turns into condition data D for adding the authentication data procedure which eliminates authentication data B by the condition data setting-out means 406, and eliminating authentication data B. Thus, two or more condition data is memorized corresponding to one authentication data.

[0050]In the register of a retail store, if the user reference part 105 is contacted in the portable information device 1, the authentication data memory measure 2 and communication are started by the authentication data reference means 112, and authentication data B will be processed with the data for authentication data discernment by the authentication data identification device 111, and it will identify. The display of the user 101 being the person himself/herself as the service use permission means 113, if authentication data B is identified is displayed on the panel of the user reference part 105, and a salesclerk is ******** to the user 101 about goods. Furthermore, accounts are settled from the user's 101 bank account. Settlement of accounts may be made when inputting authentication data into the portable information device 1. control data B including the user's 101 biological information inputted by the control data input means 8 -- the processing judging means 7 -- condition data B and **** -- last ** If the theft of the portable information device 1 is encountered during going out and it separates from the user's 101 hand, If change is produced in control data B, for example, control data B is less from a fixed pressure value, authentication data B will be eliminated by portable information device 1 inside by the authentication data erasing means 6 which operates according to the authentication data procedure added to condition data B by fulfilling the conditions of condition data B. Control data B processes condition data B by the processing judging means 7 according to condition data procedure according to control data procedure. If others communicate with the personal identification device of the retail store besides a purchase schedule, the position information on retail stores other than setting out will eliminate authentication data B by being inputted as control data C and filling condition data C. In addition, as control data D, it is inputted into the portable information device 1 by the used

amount of money for every purchase, and by the condition data alteration means 601 of drawing 6. If it is pulled from the application-limits amount of money which is the conditions of condition data D and becomes close to 0, authentication data B will be eliminated by the authentication data erasing means 4 by filling condition data D. By thus, the thing which various kinds of condition data is set up a priori, and is memorized to the portable information device 1. Authentication data B is eliminated from the portable information device 1, the outflow of the unnecessary authentication data based on a theft is prevented beforehand, the troublesomeness of management is reduced, and it becomes still more possible to utilize the storage capacity of a portable information device effectively.

[0051]

[Effect of the Invention]According to this invention, the authentication data memorized to a portable information device is eliminated arbitrarily. Therefore, the outflow of unnecessary authentication data, shortage of the storage capacity of a portable information device, etc. are prevented, and a user and a system donor can improve safety and efficiency separately.

[0052]According to this invention, the specific authentication data memorized to a portable information device is eliminated arbitrarily. Therefore, the controllability of the authentication data memorized by the portable information device by plurality is improved, and it corresponds to diversification of a personal authentication system.

[0053]According to this invention, the specific authentication data memorized to a portable information device is eliminated automatically. Therefore, by management of a portable information device, the troublesomeness in which a user manages two or more authentication data is lost, and the efficiency of a personal authentication system is improved.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]They are a portable information device of this invention, and a lineblock diagram of the personal authentication system having contained this.

[Drawing 2]It is correspondence of authentication data and condition data in this invention.

[Drawing 3]They are a portable information device of this invention, and a lineblock diagram of the personal authentication system having contained this.

[Drawing 4]They are a portable information device of this invention, and a lineblock diagram of the personal authentication system having contained this.

[Drawing 5]It is a figure showing the relation of composition required for the control data kind and control data input means of this invention.

[Drawing 6]They are a portable information device of this invention, and a lineblock diagram of the personal authentication system having contained this.

[Drawing 7]They are a portable information device of this invention, and a lineblock diagram of the personal authentication system having contained this.

[Drawing 8]It is a flow chart which shows the authentication data erasing method in the portable information device of this invention.

[Description of Notations]

1 Portable information device

2 Authentication data memory measure

3 Authentication data input means

4 Condition data memory measure

5 Condition data input means

6 Authentication data erasing means

7 Processing judging means

8 Control data input means

101 User

102 Personal identification device

103 Information transmission line

104 Information transmission line

105 User specific part

106 Information processing section

107 Authentication data reference part

108 User specifying means

109 Condition data setting-out means

110 Authentication data issuing means

111 Authentication data identification device

112 Authentication data reference means

113 Service use permission means

201 Condition data for authentication data A elimination A

202 Condition data for authentication data B elimination B

203 Authentication data B and condition data for C elimination C

204 Condition data D

205 Authentication data D

301 Personal identification device

302 Information transmission line

303 Information transmission line

304 User specific part

305 Information processing section

306 Authentication data reference part

307 Information transmission line

308 Information transmission line

309 Authentication data input means

310 Condition data input means

311 User specifying means

312 Authentication data identification device

313 Authentication data reference means

314 Control data input means

401 Information transmission line

402 Condition data input means

403 Authentication data erasure condition reporting means

404 Personal authentication possible service reporting means

405 Authentication data elimination notice means

406 Condition data setting-out means

407 Identification number memory measure

601 Condition data alteration means

701 Personal identification device

702 Wireless telephone communications network

703 Information transmission line

704 Communications department

705 Authentication data input means

706 Condition data input means

707 Control data input means

708 Communications department

709 Authentication data reference means

[Translation done.]

* NOTICES *

damages caused by the use of this translation.

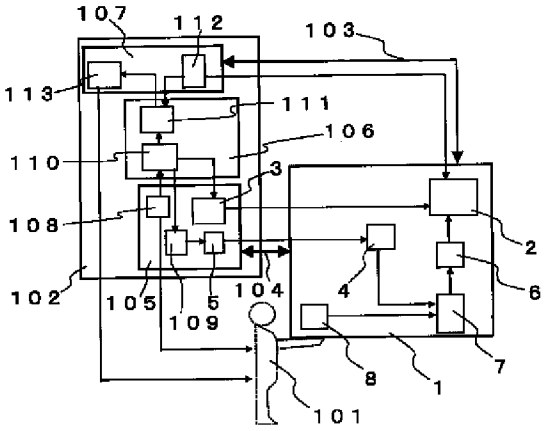
1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.

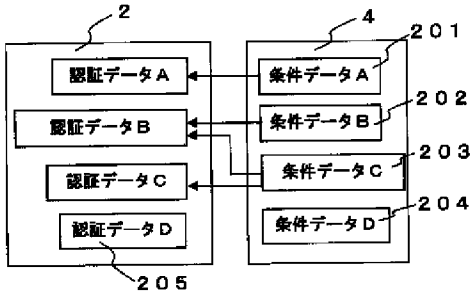
3.In the drawings, any words are not translated.

DRAWINGS

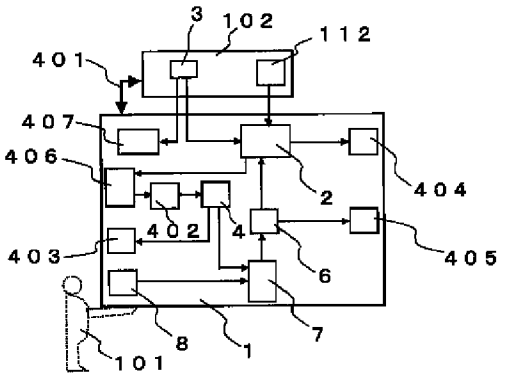
[Drawing 1]



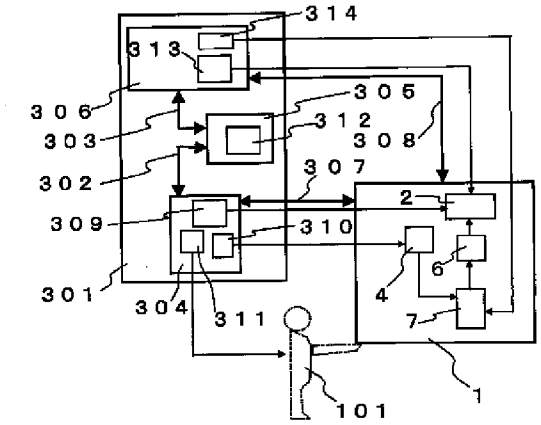
[Drawing 2]



[Drawing 4]



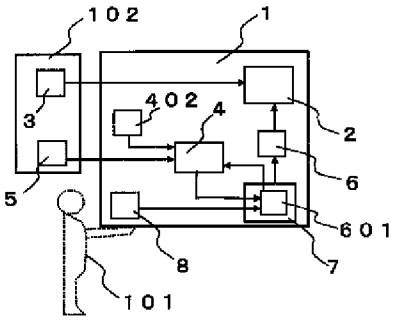
[Drawing 3]



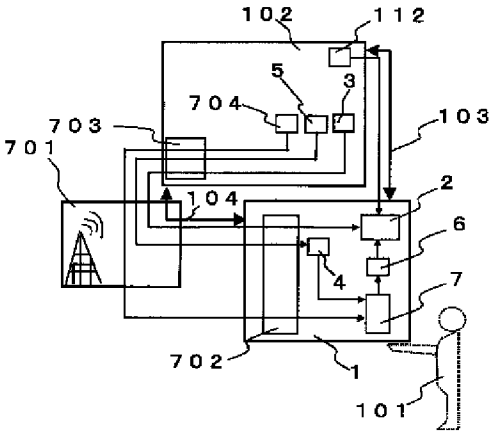
[Drawing 5]

制御データ種類	制御データ入力手段に必要な構成
外部から受信した電磁波から得る制御データ	通信部
入力部から入力する制御データ	入力部
時間情報より得る制御データ	時間情報発生部，もしくは時間情報受信部
使用者の生体情報より得る制御データ	生体情報サンプリング部
位置情報より得る制御データ	位置情報取得部
信号情報より得る制御データ	信号発生部

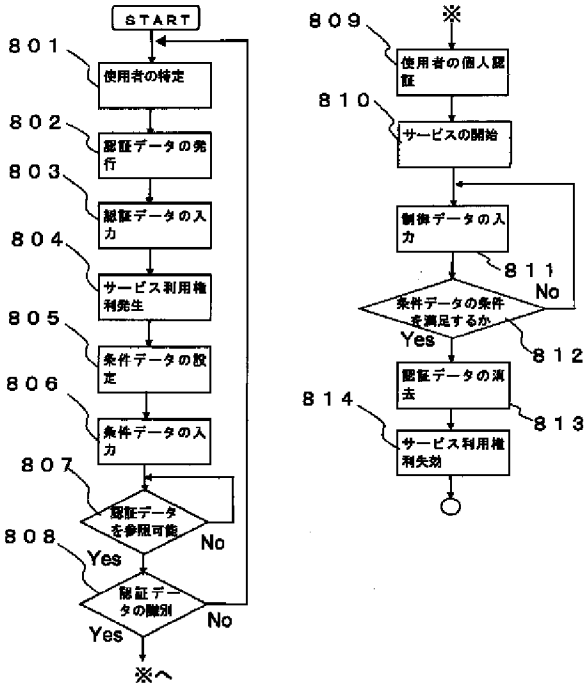
[Drawing 6]



[Drawing 7]



[Drawing 8]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－175505
（P2002－175505A）
(43)公開日　平成14年６月21日(2002.6.21)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｔ	５Ｂ０３５
			Ｖ	５Ｂ０５８
19/10		19/00	Ｒ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ	

審査請求　未請求　請求項の数25　ＯＬ　（全 16 頁）

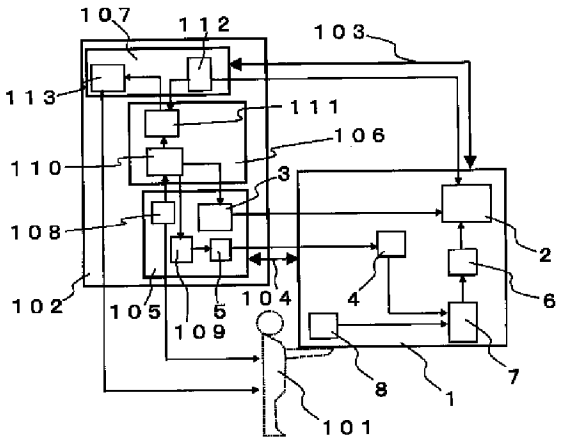
(21)出願番号　特願2000－374056(P2000－374056)
(22)出願日　平成12年12月８日(2000.12.8)

(71)出願人　000001960
シチズン時計株式会社
東京都西東京市田無町六丁目１番12号
(72)発明者　小阪　彰伯
埼玉県所沢市大字下富字武野840番地　シチズン時計株式会社技術研究所内

Ｆターム(参考)　5B035 AA13 BB09 BC01 CA38
5B058 KA01 KA12 KA33 KA37
5J104 AA07 KA01 KA15 NA05 NA35
PA02 PA10 PA11

(54)【発明の名称】　携帯型情報装置、個人認証システム及び認証データ消去方法

(57)【要約】
【課題】　個人認証システムの利用分野が多様化するにおいて、複数の認証データを個人が所持する１台の携帯型情報装置に記憶するため、管理手段の複雑化による利便性の低下や、情報装置の記憶容量不足や、認証用情報流出の危険性拡大が懸念される。
【解決手段】　認証データを消去する条件を条件データとして記憶する手段、条件データを利用して認証データを任意に消去する手段を設ける。



1

【特許請求の範囲】

【請求項１】　個人認証に利用する携帯型情報装置において、認証データを外部から入力する認証データ入力手段と、前記認証データを記憶する認証データ記憶手段と、前記認証データを消去するための条件を設定する条件データを外部もしくは内部から入力する条件データ入力手段と、前記条件データを記憶する条件データ記憶手段と、制御データを外部もしくは内部から入力する制御データ入力手段と、前記制御データと前記条件データとを処理して判定する処理判定手段と、前記認証データを消去する認証データ消去手段とを有し、前記処理判定手段の判定結果に基づいて、前記認証データを消去することを特徴とする携帯型情報装置。

【請求項２】　前記制御データ入力手段は、外部からの電磁波を受信する通信部を備え、前記制御データを外部からの電磁波により受信することを特徴とする請求項１記載の携帯型情報装置。

【請求項３】　前記制御データ入力手段は、入力ボタンもしくは入力インターフェースでデータを入力する入力部を備え、前記制御データを前記入力部から入力することを特徴とする請求項１記載の携帯型情報装置。

【請求項４】　前記制御データ入力手段は、時間情報を得る時間情報発生部もしくは外部から時間情報を得る時間情報受信部を備え、前記制御データを前記時間情報より得ることを特徴とする請求項１記載の携帯型情報装置。

【請求項５】　前記制御データ入力手段は、生体情報を得る生体情報サンプリング部を備え、前記制御データを使用者の前記生体情報より得ることを特徴とする請求項１記載の携帯型情報装置。

【請求項６】　前記制御データ入力手段は、位置情報を得る位置情報取得部を備え、前記制御データを前記位置情報より得ることを特徴とする請求項１記載の携帯型情報装置。

【請求項７】　前記制御データ入力手段は、センサーを備える信号出力部を備え、前記制御データを前記信号出力部で発生する信号より得ることを特徴とする請求項１記載の携帯型情報装置。

【請求項８】　前記制御データ入力手段は、内蔵する発電手段もしくは内蔵する充電手段による信号出力部を備え、前記制御データを前記信号出力部で発生する信号より得ることを特徴とする請求項１記載の携帯型情報装置。

【請求項９】　前記処理判定手段は、前記制御データにより前記条件データを変更する条件データ変更手段を有し、前記制御データの入力により変更された条件データが指定の条件を満たすことで前記認証データを消去することを特徴とする請求項１記載の携帯型情報装置。

【請求項１０】　前記認証データ記憶手段は、記憶する認証データが個人認証するのに必要なデータの一部であることを特徴とする請求項１記載の携帯型情報装置。

2

【請求項１１】　前記認証データ記憶手段は、２つ以上の認証データを記憶することを特徴とする請求項１記載の携帯型情報装置。

【請求項１２】　前記条件データ記憶手段は、複数の認証データを消去するための１つの条件データを記憶することを特徴とする請求項１記載の携帯型情報装置。

【請求項１３】　前記条件データ記憶手段は、１つの認証データを消去するための複数の条件データを記憶することを特徴とする請求項１記載の携帯型情報装置。

【請求項１４】　前記認証データをどのような条件で消去するか使用者へ知らせる認証データ消去条件通知手段を備えることを特徴とする請求項１記載の携帯型情報装置。

【請求項１５】　現状記憶している認証データにより個人認証して利用可能なサービスを音声もしくは表示で使用者へ知らせる個人認証可能サービス通知手段を備えることを特徴とする請求項１記載の携帯型情報装置。

【請求項１６】　前記認証データを消去することを使用者へ予告する認証データ消去予告手段を備えることを特徴とする請求項１記載の携帯型情報装置。

【請求項１７】　識別番号を記憶する識別番号記憶手段を備えることを特徴とする請求項１記載の携帯型情報装置。

【請求項１８】　電話網接続手段、インターネット網接続手段のうちの少なくとも一方を備えることを特徴とする請求項１記載の携帯型情報装置。

【請求項１９】　前記認証データ消去手段は、外部の電磁場もしくは外部の電磁波を利用して消去することを特徴とする請求項１記載の携帯型情報装置。

【請求項２０】　前記条件データ記憶手段に記憶するための前記条件データを設定する条件データ設定手段を備えることを特徴とする請求項１記載の携帯型情報装置。

【請求項２１】　使用者を特定する使用者特定手段と、後で識別可能な認証データを発行する認証データ発行手段と、前記認証データを請求項１から請求項２０に記載の携帯型情報装置へ入力する認証データ入力手段と、前記携帯型情報装置に記憶する認証データを参照する認証データ参照手段と、前記認証データを識別する認証データ識別手段と、サービス利用を許可するサービス利用許可手段とを備える個人認証装置と、前記携帯型情報装置と前記個人認証装置との有線、無線もしくは接触による情報伝送路とを備え、前記個人認証装置が特定した使用者の指定する前記携帯型情報装置へ前記認証データを入力し、その後前記個人認証装置が前記認証データを参照し、前記認証データを識別することで使用者の個人認証を行い、サービスの利用を許可することを特徴とする個人認証システム。

【請求項２２】　前記個人認証装置は、条件データを設定する条件データ設定手段と、条件データを前記携帯型

情報装置へ入力する条件データ入力手段とを有し、前記個人認証装置において設定した条件データを前記携帯型情報装置へ入力し前記携帯型情報装置が条件データを記憶した後に入力する制御データと前記条件データを前記携帯型情報装置内で処理して判定した結果に基づいて、前記認証データを消去することを特徴とする請求項２１記載の個人認証システム。

【請求項２３】　前記個人認証装置は、少なくとも使用者特定手段と認証データ入力手段とを有する使用者特定部と、少なくとも認証データ識別手段を有する情報処理部と、少なくとも認証データ参照手段を有する認証データ参照部と、使用者特定部と情報処理部と認証データ参照部との有線もしくは無線の情報伝送路とを備え、認証データ参照部は，携帯型情報装置との有線、無線もしくは接触による情報伝送路を備え、前記使用者特定部は，前記携帯型情報装置と有線、無線もしくは接触による情報伝送路とを備え、使用者特定部が特定した使用者の指定する前記携帯型情報装置へ前記認証データを入力し、前記認証データを認証データ参照部が参照した後に前記情報処理部が前記認証データを識別することによって、使用者のサービス利用を許可することを特徴とする請求項２１記載の個人認証システム。

【請求項２４】　前記使用者特定部は、条件データ設定手段と、条件データ入力手段とを備えることを特徴とする請求項２３記載の個人認証システム。

【請求項２５】　個人認証用の携帯型情報装置で利用する認証データ消去方法において、請求項１から請求項２０のいずれか１項に記載の携帯型情報装置に認証データと前記認証データに対応した条件とを入力して記憶し、前記条件を満足する信号を前記携帯型情報装置が識別することにより前記認証データを消去する認証データ消去方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、入門や、改札や、コンピュータへのログオンや、クレジット処理や、キャッシングや、商品売買や、レンタル機器利用などのサービスに利用される個人認証システムで使用する携帯型情報装置に関するものであり、個人認証システムのシステム提供者や使用者にとって特に個人認証システムの安全性や、効率性を高めることを実現する個人認証用の携帯型情報装置、個人認証システム及び認証データ消去方法に関するものである。

【０００２】

【従来の技術】個人認証システムはサービスを利用する際に、許可された正当な使用者であることを確認するセキュリティシステムである。入門、改札、コンピュタへのログオン、クレジット処理、キャッシング、商品売買、レンタル機器利用などのサービスを管理する情報処理システムで使用者の認証をすることを、個人認証をするという。使用者の認証とは、情報処理システムのセキュリティ対策として、情報処理ハンドブック（１９８９年　第１版　情報処理学会編）に記載の外部セキュリティと、内部セキリュティと、使用者の認証の内、許可された正当な使用者であることを確認する使用者の認証である。最も普及している利用方法は、入門、商品購入、コンピュータへのログインなどの際に、本人しか持っていないものをシステムを管理する装置が参照することで、使用者を使用者本人であると認定し、サービスをうけることが可能となるものである。現在、パスワードや、クレジットカードを利用する方法が一般的である。しかし、これらの個人認証方法は、本来の使用者であることを特定する手段が少なく、他人に使われやすく安全性に問題がある。しかし、その利便性から、個人認証システムを利用するサービスは社会に広がっており、インターネットを利用した電子商取引ではさらに個人認証システムの安全性が問われている。

【０００３】近年、比較的大きな記憶容量を有するＩＣカードを利用してパスワードなどを複雑なデータに置き換えて利用する個人認証方法が普及始めている。例えばカード内に記憶する個人の生体情報を含むデータと、認証する現場で実際に取得した生体情報とを、処理し、一致するか否か判定して個人認証する安全性の高く、汎用性ある個人認証システムが考案されている。個人認証に必要とするデータを認証データと呼ぶと、ＩＣカードを利用した認証方法は、大量の個人情報を含む認証データが１枚の記憶媒体に記憶されていることで、正当な使用者であると判定する。個人しか持ち得ない生体的特徴を利用するという前提の下、比較的簡便かつ安全性や、信頼性の高い方法である。また、インターネットに接続する携帯電話など携帯型情報装置の普及により、認証データをこれらに記憶させ外出先にて個人認証する利用方法も考えられている。使用者が日常携帯する携帯型情報装置を複数の個人認証システムで利用することで使用者の利便性は向上し複数のカードを所持したり、複数のパスワードを頭に記憶する不便さから解放される。システムを提供する側も複数の携帯型情報装置をデータ通信により素早く個人認証することにより複数の使用者が利用するシステムについて効率化をはかることが可能となる。しかし、携帯型情報装置を利用した個人認証システムの普及と同時に、携帯型情報装置の紛失により詳細かつ大量の個人情報や、変更不可能な個人の身体的特徴の情報を流出する危険性があり、安全性に課題を生じる可能性も高い。また、データで個人認証するために古い認証データを新しい認証データに頻繁に更新して安全性を確保する必要も生じるとともに効率的な認証データの管理も必要となる。

【０００４】ＩＣカードや携帯型情報装置などにおいて、認証データを消去したり、使用不可能にして安全性を確保する方法が考案されて入れいる。認証データと

5

は、個人認証システムで使用を許可された使用者と使用を許可されていない者、もしくは他の使用者とを識別して個人認証するのに利用するデータで、発行の後に識別する手段を有する。例えば、暗号化などの複製防止や不正利用防止の内部セキュリティ制御がなされ、パスワード情報や、署名などの行動による情報や、バイオメトリクスなど生物学的情報や、記憶媒体から読みとった情報や、商品売買証明情報を含み、これらを所持することで使用者本人を識別する。また、発行後に識別する手段とは、例えば暗号技術を使用した電子鍵や、電子鍵の一部などを利用すればよい。利用方法としては、使用者が認証データをあらかじめ記憶した携帯型情報装置をサービスを受ける現場へ携帯し、システム提供者の管理する装置が認証データを識別すると、使用者はサービスの利用を許可される。システム提供者とは個人認証システムを利用してサービスを使用者へ提供する者や組織である。データであることから１つの携帯型情報装置に複数記憶したり、都合良く消去したり、新しいものに更新可能である。さらに、認証データを参照するだけで個人認証するシステムは利用者が多い現場での迅速な認証が可能となる。

【０００５】ＩＣカードの不正使用防止装置（特願平８－２７４１３６）は、ＩＣカードに無線信号を受信する受信部と、所有者を識別するためのデータを記憶する記憶部を有し、受信部に所定の無線信号が所定時間受信できないときに、記憶部に記憶した認証データを消去又は使用不可能にする。これにより、ＩＣカードを紛失したり盗難に遭ったときに速やかに使用できなくする。また、個人認証システムの情報装置及び入力装置（特願平１１－２８２９８１）は、携帯型情報装置に人体装着状態を検出する手段を有し、使用者からの携帯型情報装置の離脱を検知すると、携帯型情報装置に格納した認証データを使用不可能にする。これらは、安全性については考えられているが、ＩＣカードや携帯型情報装置に備わる構成により単純に認証データが消去され、使用者やシステム提供者が特定の認証データを任意に消去するなど利便性の向上は困難である。さらに、複数記憶した認証データを個々に対して安全性を向上することについて記載されておらず、認証データの効率的管理や、携帯型情報装置の記憶容量の有効利用や、個人認証システムの利用分野の多様化には対応困難である。

【０００６】

【発明が解決しようとする課題】上述のように、個人認証システムの利用分野が多様化するにおいて、効率性と、安全性に新たな問題が生じることが考えられる。特に、複数の認証データを、個人が所有する１つの携帯型情報装置に記憶し、複数のサービス現場で利用するのに認証に利用するデータの管理手段の複雑化による利便性の低下や、利用後に不必要な認証データが残ることで携帯型情報装置の記憶容量の不足や認証用情報流出の危険

6

性拡大とから、システムの効率性と、安全性に課題を生じる。

【０００７】本発明は前記問題点に鑑みてなされたもので、特に、個人認証システムの効率性と、安全性をサービス提供者や使用者が個々に高める携帯型情報装置を提供することを目的とする。また、本出願は、新規な機能を有し、安全性と、効率性を高める携帯型情報装置、個人認証システム及び認証データ消去方法を提供することを他の目的とする。

【０００８】

【課題を解決するための手段】個人認証に利用する携帯型情報装置において、認証データを外部から入力する認証データ入力手段と、認証データを記憶する認証データ記憶手段と、認証データを消去するための条件を設定する条件データを外部もしくは内部から入力する条件データ入力手段と、条件データを記憶する条件データ記憶手段と、制御データを外部もしくは内部から入力する制御データ入力手段と、制御データと条件データとを処理して判定する処理判定手段と、認証データを消去する認証データ消去手段とを有し、処理判定手段の判定結果に基づいて、認証データを消去する。

【０００９】このような構成を携帯型情報装置が備えることにより、システム提供者や、使用者が認証データを消去する条件を任意に設定し、前もって入力しておくことで、条件を満足した時点で記憶する複数の認証データから特定の認証データを消去することで、個々の認証データに制御性を付加し、個別管理が可能となることで、不必要な流出を防ぎ安全性を確保する。さらに、携帯型情報装置の記憶容量確保や、認証データの管理にわずらわされなくなり、利便性を向上することで、効率性を確保することが可能となる。

【００１０】

【発明の実施の形態】（実施例１）図１は本発明のシステム構成を示す図である。使用者が認証データをあらかじめ記憶した携帯型情報装置をサービスを受ける現場へ携帯し、システム提供者の管理する装置が認証データを識別すると、使用者はサービスの利用を許可される。このような個人認証システムの利用分野が多様化するにおいて、１つの携帯型情報装置を共用して利用するのに個人認証システムの効率性と、安全性に新たな問題が生じることが考えられる。つまり、１つの携帯型情報装置に複数の認証データを記憶して利用する場合において、使用者は携帯型情報装置の記憶容量確保や、認証データの管理にわずらわされるなど効率性の低下が考えられるほか、携帯型情報装置の盗難などにより個人情報を含んだ認証データの流出頻度が多くなるという安全性に課題がある。

【００１１】本発明では、システム提供者や、使用者が認証データを消去する条件を任意に設定し、前もって携帯型情報装置へ入力しておくことで、条件を満足した時

点で携帯型情報装置内に記憶する複数の認証データから特定の認証データを消去し、個々の認証データに制御性を付加し、個別管理が可能となる。これにより、盗難時に使用後の認証データを携帯型情報装置内に記憶していたためになされる不必要な情報流出を防止する。さらに、目的に応じて認証データを大きく複雑にして安全性を高めたり、複数の認証データを利用するが利用後自動的に消去することで、携帯型情報装置の記憶容量を効率よく確保し、さらに複数の認証データを利用するのに管理の煩わしさを使用者が受けることがなくなり、さらに常に新しい認証データに更新して利用するのが可能となる。このように、１つの携帯型情報装置を複数の個人認証システムで利用したり、データの通信のみで個人認証するなど個人認証システムの利用分野の多様化に対応し、使用者及びシステム管理者にとって安全性と、効率性に優れた携帯型情報装置と、個人認証システムと、認証データ消去方法とを提供する。

【００１２】図１は、携帯型情報装置１と、個人認証装置１０２と、使用者１０１と、携帯型情報装置１と個人認証装置１０２との情報伝送路１０３、１０４とからなる。さらに、個人認証装置１０２は使用者特定部１０５と、情報処理部１０６と、認証データ参照部１０７を有し、使用者特定部１０５は携帯型情報装置１と情報伝送路１０４で通信し、使用者参照部１１３は携帯型情報装置１と情報伝送路１０３で通信する。個人認証装置１０２をこのような構成にすることで、家庭のドアの内側に使用者特定部１０５と情報処理部１０６を設置し、ドアの外側に認証データ参照部１０７だけを設置して個人認証システムの安全性を確保するなどシステムの多様化に対応する。また使用者特定部１０５と情報処理部１０６と認証データ参照部１０７を分離して複数台設置しそれぞれを情報伝送路で接続して１つの装置として利用してもよい。図１の１は携帯型情報装置で、個人が携帯するよう軽量化、省電力化されている。主に携帯電話や、ＰＨＳや、携帯型コンピュータや、腕時計や、腕時計型情報機器や、携帯型情報末端や、携帯型ゲーム機や、ＩＣカードを差し込んで機能する携帯型機器や、これら機器を複合化した機器であり、携帯型情報装置１が認証データを記憶していることで、サービスを受ける現場にて個人認証し、使用者１０１はサービスを受けることを許可される。２は認証データ記憶手段で、認証データを記憶する。記憶装置は半導体素子や、磁気ドライブや、光ディスクなど各種あるが、安全に認証データを記憶することを重視し、個人認証システムの気密性を考慮し、携帯型情報装置１の省電力性や、軽量性や、耐久性や、コストにより選択すればよい。配布が容易なＩＣカードなど記憶媒体をカセットやカードのように携帯型情報装置１に差し込んで記憶媒体としてもよい。記憶装置により電気や、磁気や、光などを利用して記憶する。３は認証データ入力手段で、携帯型情報装置１外部から入力する。

【００１３】図１では、使用者特定部１０５から携帯型情報装置１へ情報伝送路１０４により入力する。認証データで使用者１０１と携帯型情報装置１を対応させるために、特定した使用者１０１が指定する特定の携帯型情報装置１へ入力する必要がある。携帯型情報装置１の特定方法は、使用者１０１の特定時に参照した固有の識別番号による携帯型情報装置１の特定方法や、使用者１０１の特定時に使用者特定部１０９と情報伝送路１０４で通信している携帯型情報装置１へ入力する方法や、使用者１０１特定において使用者特定部１０９へ接続し離脱を確認していない特定の携帯型情報装置１へ入力する方法などがある。

【００１４】４は条件データ記憶手段で、特定の認証データを消去するのに利用するため条件データを携帯型情報装置１内に記憶する。認証データと同様な方法で記憶され、記憶装置は同一であってもよいが、条件データを処理することから自由に読み出し可能である。条件データとは、処理可能なデータであり、少なくとも、対応する特定の認証データを消去する条件を含み、条件を満足すると、携帯型情報装置１内の特定の認証データは消去される。携帯型情報装置１内で認証データを消去するために、条件の他に、特定の認証データを消去する認証データ処理手順や、条件を満たしたかどうかを処理し判定する条件データ処理手順を含むプログラムを条件データに含めてよい。その他に条件データは認証データを消去するために任意に入力する特定の制御データと処理する制御データ処理手順を付加したり、条件データは認証データと同時に消去されてよいため使用後に条件データを消去する手順を条件データ処理手順に含めてもよい。条件データに含まれる条件や手順などのプログラムは携帯型情報装置１の制御データ入力手段８や外部からの制御データ入力手段７０７により入力される制御データの種類にあわせて内容を設定する必要がある。例えば、認証データを入力し記憶する前後に携帯型情報装置１、もしくは個人認証装置７０１が有する制御データ入力手段８、７０７を確認し特定の制御データを処理するよう制御データ処理手順を自動的に付加し、さらに制御データにふさわしい条件を使用者１０１などが設定し付加する。その他に自由に消去できない認証データを認証データ処理手順を利用することによって消去してもよい。５は条件データ入力手段で、携帯型情報装置１外部から入力する。条件データは携帯型情報装置１内部で入力してもよい。

【００１５】図１では、外部である使用者特定部１０５から情報伝送路１０４により認証データと同時又は前後に入力する。６は認証データ消去手段で、処理判定手段７による認証データを消去する判定後に認証データ記憶手段２で記憶する認証データを消去する。半導体素子や磁気ドライブのように記憶装置単体で消去できるものは携帯型情報装置１内部に全て消去機構がある。外部の電

磁場や外部の電磁波を利用して消去するには、携帯型情報装置１の外部のみ、もしくは外部と内部の構成を組み合わせて消去する。例えば，個人認証装置１０２の発する電磁場へ携帯型情報装置１をかざすことで認証データを消去する磁気カードのような消去方法や、紫外線を携帯型情報装置１に照射することで認証データを消去する消去方法を利用してもよい。消去とは、認証データを携帯型情報装置１からあらゆる手段を使用しても読み出せないよう、情報を消したり、他の情報で上書きすることで、実施例では、消去により、個人認証不可能となり、つまり、使用者１０１のみならず、携帯型情報装置１を盗すんだ犯罪者もサービス利用が許可されない。さらに、条件データを満足した後に自動で消去することにより、携帯型情報装置１の記憶容量を効率よく確保したり、使用者１０１がサービス利用後消去する手間も省ける。

【００１６】７は処理判定手段で、条件データや制御データを処理して判定する。処理とは必要な情報を得るためにデータに対して行う一連の作業である。例えば、データを読み込んだり、データを作成したり、データを消去したり、データを補正したり、データが他のデータを識別したり、データと他のデータを照合又は比較したり、照合又は比較する前にデータの変化量や、誤差量や、一定値や、平均値を算出したり、照合又は比較した結果一致したか否の結果を得ることである。処理判定手段７における必要な情報とは認証データを消去するか否かの情報である。本実施例では特に、入力した制御データと先に記憶する条件データとを処理し、主に制御データが条件を満たすもしくは満たさないことにより、認証データを消去するか否かの情報を得たことを判定する。８は制御データ入力手段で、制御データとは、認証データを消去するきっかけとなるデータで、修理する手順を制御データ処理手順などとして条件データに含めてよい。本実施例では特に条件データの条件を満足するデータを制御データとして携帯情報装置１内へ入力し条件データと処理することにより、特定の認証データを消去する。必要なときだけ入力しても、切れ間なく入力しても、断続的に入力してもよく、認証データの種類や携帯型情報装置１の構成により選択すればよい。例えば電磁波により受信する制御データは受信したときのみ入力すればよく、生体情報による制御データは使用者１０１の生体情報を定期的にサンプリングしたデータである制御データの変化量が条件を満たすか知るために断続的な入力が必要である。図１では携帯型情報装置１内部で入力する。制御データは図５に示すとおり複数の種類がある。

【００１７】１０２は個人認証装置で、特定した使用者１０１の特定の携帯型情報装置１へ認証データを入力し、後にサービス現場で、携帯型情報装置１に記憶する認証データを参照し識別することで、個人認証する装置である。このとき、使用者１０１を特定する使用者特定手段１０８と、後で識別可能な認証データを発行する認証データ発行手段１１０と、認証データ入力手段３と、携帯型情報装置１に記憶する認証データを参照する認証データ参照手段１１２と、正当な認証データか識別する認証データ識別手段１１１と、サービス利用を許可するサービス利用許可手段１１３を備える。個人認証装置１０２がこれら手段を有することで、携帯型情報装置１を利用して使用者１０１とその他使用者や使用を許可していない者とをサービス現場にて識別する。

【００１８】１０５は使用者特定部で、少なくとも使用者特定手段１０８と、認証データ入力手段３とを有し、その他に条件データ入力手段５や条件データ設定手段１０９を有すると使用者１０１がその場で画面を見ながら条件を選択するなど事前に認証データを自動的に消去する準備ができ利便性が向上する。使用者特定手段１０８は、認証データを利用する使用者１０１が、システム提供者に許可された正当な使用者であることを特定し、例えば集金が可能なことを確認する。使用者の特定を始めることにより、使用者１０１と後に使用する認証データを対応させ個人認証システムの利用を開始する。使用者１０１の特定方法としては、パスワードを知っていること、もしくは、所有する携帯型情報装置１の識別番号、もしくは、暗証番号を利用し使用者を特定する方法や、その外に、コンピュータや、コンビニエンスストアの大型の末端などに使用者特定部１０５を設置し、バイオメトリクスなど生物学的情報を測定し、過去の測定データと照合する方法など、各種信頼性の高い方法を利用したり、クレジッタカード、ＩＣカードなど記憶媒体による特定、単に商品や利用権利を購入した者としての特定など、利便性のある方法、いずれも必要な効率性、信頼性で選択すればよい。条件データ設定手段１０９は、少なくとも設定する必要のある条件の外に、認証データ処理手順や、条件データ処理手順や、制御データ処理手順などを手順により自動、もしくは、使用者１０１やシステム提供者が設定する。例えば、制御データ処理手順は携帯型情報装置１が有する制御データ入力手段８の種類により自動的に設定され、条件は使用者特定部３０１上のパネルからシステム提供者があらかじめ設定した複数の条件から使用者１０１が選択することで設定される。

【００１９】１０６は情報処理部で、少なくとも認証データ識別手段１１１を有し、コンピュータなどで利用状況など個人情報をデータベース化し管理していてもよい。この時、認証データ発行手段１１０も有して発行した認証データや認証データ識別用データもデータベース内で一元管理してもよい。認証データ発行手段１１０は使用者１０１の特定と携帯型情報装置１の特定が確かである間に、後で識別可能な認証データを発行する。認証データ識別手段１１１による認証データの識別方法は、認証データ発行手段１１０により電子鍵のように個人認

証するのに必要な一部を認証データとして携帯型情報装置１０１へ入力し、他の一部である認証データ識別用データを同時に発行し、個人認証する時に携帯型情報装置１で参照した認証データを認証データ識別手段１１１で利用してもよい。その他の方法として、認証データ発行手段１１０において使用者１０１を特定するための情報や携帯型情報装置１の識別番号を認証データに含ませて発行し、個人認証時に再度使用者１０１や携帯型情報装置１の特定を行い認証データ識別手段１１１で利用する方法などがあり、システムの構成などにより適した認証データの発行方法を利用すればよい。

【００２０】１０７は認証データ参照部で少なくとも認証データ参照手段１１２を有し、その他にサービス利用許可手段１１３を有してもよい。認証データ参照手段１１２は携帯型情報装置１に記憶する認証データを情報伝送路１０３を利用して参照する。参照とは認証データ記憶手段２に記憶する認証データを識別する情報を得るために行う一連の作業であり、認証データ記憶手段２へのデータ送受信手段の確立や、データの検出や、データの存在の確認や、データの読み取りや、比較又は照合する一連の作業である。情報伝送路１０３と情報伝送路１０４は同じ通信方法でもよい。携帯型情報装置１が無線携帯電話接続手段やインターネット接続手段を有してこれを利用して通信したり、近距離無線通信や赤外線など電磁波を利用して通信したり、有線により接続したり、装置同士を接触することで通信するようにして認証データの流出を極力抑えてもよい。サービス利用許可手段１１３は、参照した認証データを使用者１０１の特定時に発行した正当な認証データと識別するとサービスを利用を許可する。例えば、改札や入門ならばドアが開いたり、商品の受け渡しならば本人であることを表示したり、コンピュータのログオンがなされたりしてサービスを受ける。このように、ドアの開鍵、開閉、乗り物の改札、コンピュータの動作開始、コンピュータによる個人署名入力、コンピュータによる契約書送付、使用者本人であることの証明表示、商品購入の精算、現金の預け入れ、現金の支払い、現金の払い戻し、機器の動作開始など利用分野による。

【００２１】図２は、携帯型情報装置に記憶する認証データと条件データの対応，図３は携帯型情報装置とこれを含んだ個人認証システムの構成図、図４は携帯型情報装置とこれを含んだ個人認証システムの構成図、図５は制御データ種類と制御データ入力手段に必要な構成の関係を示した図、図６は携帯型情報装置の詳細を示した個人認証システムの構成図、図７は図３は携帯型情報装置とこれを含んだ個人認証システムの構成図である。

【００２２】図２は携帯型情報装置１に記憶する認証データと条件データの対応を示したものである。携帯型情報装置１が複数の認証データを記憶することで、使用者１０１は複数の個人認証システムを利用する。認証データＡは個人認証システムＡで、認証データＢは個人認証システムＢで、認証データＣは個人認証システムＣで個人認証に使用する。また、認証データＡと認証データＤを揃えると、個人認証システムＤで個人認証をする利用方法もよい。個人認証システムＡからＤはそれぞれ独自の個人認証装置を備えており，別々のシステム提供者が管理してよい。図中で認証データの大きさが異なるが，認証データの大きさを表す。内部セキュリティが十分になされたデータは一般的に大きくなるが，全ての個人認証システムで大きい認証データを利用する必要とする訳ではなくサービス提供者が必要に応じて選択すればよい。条件データも含む条件や手順によってその大きさも異なる。

【００２３】条件データＡは認証データＡを消去する目的で記憶しており、条件データＡの条件を満足すると認証データＡのみを携帯型情報装置１より消去する。認証データＢは条件データＢの条件を満足すると消去されるが、条件データＣの条件を満足しても消去される。条件データＣの条件を満足すると認証データＢとともに、認証データＣも消去される。認証データＤは認証データ入力後、使用者１０１が携帯型情報装置１上で条件データを設定するため対応する条件データが存在しない。また、重要でない認証データでは従来と同様に条件データを設定しないでもよい。条件データＤは携帯型情報装置１の出荷時にすでに入力されている条件データで、使用者１０１は携帯型情報装置１上で記憶する特定の認証データを消去するよう設定する。携帯型情報装置１が備える制御データ入力手段８の種類と合わせて条件データを事前に用意することで操作性が向上する。

【００２４】図３は図１の個人認証システムとは異なるシステム提供者が提供する個人認証システムの構成図である。使用者１０１が利用する携帯型情報装置１は同じである。この個人認証システムでは個人認証装置１０２と異なる個人認証装置３０１を利用するが有する手段は個人認証装置１０２と同様である。異なるのは使用者特定部３０４と情報処理部３０５と認証データ参照部３０６を分離して別の場所に設置する点である。それぞれ所有者は異なってもよいが、個人認証するのに１つの装置として動作する。使用者特定部３０４と情報処理部３０５と認証データ参照部３０６はそれぞれ情報伝送路３０２、３０３で接続してある。例えば使用者特定部３０４を個人宅に配置し、認証データ参照部３０６をサービス現場の小売店などに配置し、情報処理部３０５をシステム提供者の会社に配置することで、システムの多様化に対応しやすくなる。使用者特定部３０４や認証データ参照部３０６は複数存在してもよく、少なくとも１つの情報処理部３０５で一元管理する。使用者特定部３０４は少なくとも使用者特定手段３１１と認証データ入力手段３０９を、情報処理部３０５は少なくとも認証データ識別手段３１２を、認証データ参照部３０６は少なくとも

認証データ参照手段３１３を有する。図３では使用者特定部３０４はさらに条件入力手段３１０を有し、認証データ参照部３０６はさらに制御データ入力手段３１４を有する。図１の個人認証装置１０２が有する条件データ設定手段１０９や、認証データ発行手段１１０や、サービス利用許可手段１１３などと同様な手段は個人認証装置３０１のどこに内蔵してよく利用する情報伝送路やシステムの運用方法により選択すればよい。ただし、個人認証装置３０６は、システム提供者が充分管理する装置、もしくは希望したレベルで認定された装置である必要がある。例えば、個人宅に設置する使用者特定部３０６がシステム提供者にとり信頼性のないものであれば、認証データの信頼性も失われる。

【００２５】図４は携帯型情報装置の詳細図である。図４では携帯型情報装置１の識別番号記憶手段４０７に記憶する識別番号を利用して、特定した使用者１０１の携帯型情報装置１を複数の携帯型情報装置より特定し、認証データを入力する。識別番号はこれにより携帯型情報装置１を特定可能な番号であり，携帯型情報装置１が有線電話接続手段や無線電話接続手段や有するなら電話番号やこれに準ずるものであり、インターネット接続手段を有するならアドレス番号やこれに準ずるものである。システム提供者に信頼のある識別番号を利用することで集金も効率的に行うことが可能となる。

【００２６】条件データ入力手段４０２は、条件データ入力手段５のように携帯型情報装置１外部である個人認証装置１０２から入力する方法の他の入力方法として、携帯型情報装置１内部で条件データを入力する方法である。同時に、携帯型情報装置１は条件データ設定手段４０６を有し、記憶している複数の認証データから消去する認証データを特定し、どのような条件で消去するか自動的に、もしくは使用者１０１が設定する。条件の他に認証データ処理手順や、条件データ処理手順を含むプログラムや、制御データ処理手順や、条件データ消去手順を付加する。特に携帯型情報装置１が備える制御データ入力手段８に合わせて条件データを設定する必要がある。携帯型情報装置１の出荷時に条件や条件データ処理手順や制御データ処理手順をいくつか設定しておき認証データを記憶した後に認証データ処理手順を設定して条件データとして入力する方法もある。

【００２７】その外に、携帯型情報装置１は使用者１０１へ次のことを通知する手段を有してよい。記憶する認証データをどのような条件で消去するか通知する認証データ消去条件通知手段４０３や、記憶する認証データがどの個人認証システムで個人認証可能か通知する個人認証可能サービス通知手段４０４や、認証データを消去する予告をする認証データ消去予告手段４０５など。これら手段を携帯型情報装置１が有することで携帯型情報装置を利用した個人認証システムにおける使用者１０１の利便性は向上する。

【００２８】図５は制御データ種類と制御データ入力手段に必要な構成を示す。制御データ入力手段は記載した構成から制御データを入力する。入力手段は図１のように携帯型情報装置１内の制御データ入力手段８、図７のように携帯型情報装置１外部からの制御データ入力手段７０７がある。制御データの種類は、外部から受信した電磁波よりえる制御データや、入力部より入力する制御データや、時間情報よりえる制御データや、生体情報によりえる制御データや、信号情報によりえる制御データがある。以下にそれぞれ説明する。

【００２９】外部から受信した電磁波よりえる制御データは、無線電話網や近距離通信方法などを利用し電磁波を利用して入力する。携帯型情報装置１外部から入力する、もしくは携帯型情報装置１に備わる通信部から入力することになる。例えばシステム提供者が通信可能エリア内で任意に認証データを消去することが可能となる。制御データＡを受信することで認証データＡを消去するならば、システム提供者が個人認証装置１０２から制御データＡと処理する認証データＡに対応した条件データＡを事前に入力しておく。入力部から入力する制御データは携帯型情報装置１に備わる入力ボタン、入力インターフェースから使用者１０１や、システム提供者が入力し、任意に消去するのに利用する。時間情報によりえる制御データは携帯型情報装置１に備わる時間情報発生部からの入力で、日付、時間により任意に消去する。生体情報によりえる制御データは、携帯型情報装置１に備わる生体情報サンプリング部からの入力で使用者１０１が死亡、体調不良などを感知して消去する。位置情報によりえる制御データは携帯型情報装置１に備わる位置情報取得部からの入力で広大な位置情報によりある位置を超えると消去する。信号情報によりえる制御データは、携帯型情報装置１に備わるセンサー部からの入力で、他の人間が接触、情報装置を脱着、体調不良を感知すると消去する。例えば、携帯型情報装置１のおかれた状況を示す温度センサーや、圧力センサーや、湿度センサーや、気圧センサーや、フォトセンサーや、圧力センサーや、イメージセンサーや、バイオセンサーや、磁気センサーや、距離センサーなど、使用者１０１の体温、生体パルス、脈拍、体液成分、血流などに関連した生体パラメータ測定機構や、体温などで発電している電流値や電圧値を測定する、各種センサーである。携帯型情報装置１が状況を直接測定する手段を有し、条件データにより任意に認証データを消去する条件を設定することにより認証現場での使用者１０１や携帯型情報装置１の状況にそくした認証データ流出防止により安全性を向上する。

【００３０】実施例では携帯型情報装置１が認証データ入力手段８として時間情報発生部を有し、制御データを時間情報により入力する制御データ入力手段８、さらに通信部を有し、制御データは個人認証装置１０２から制御データ入力手段７０７により携帯型情報装置１へ入力

する。

【００３１】図６は認証データ消去方法の構成図を示す。条件データを変化させ最終的に認証データを消去する構成である。携帯型情報装置１は条件データ変更手段６０１を有すればよく、例えば、制御データ入力手段８として入力部により制御データを入力することにより、条件データを変更する。その外に、条件データがサービス利用限界数の情報を含み、制御データ入力手段８でサービス利用ごとに制御データを入力し、処理判定手段７の条件データ変更手段６０１により前記サービス利用限界数を減算して０になると条件を満たした判定をし、認証データ消去手段６により特定の認証データを消去するなど、携帯型情報装置１を利用して、回数券や、プリペードカードのような利用を可能とする。

【００３２】図７は、実施例１の認証データ消去方法の構成図を示す。通信部７０２よりの制御データの入力とすると図１と同様な認証データ消去システム構成になるが、制御データ入力手段７０４が個人認証装置１０２に有するとし電磁波による制御データの入力元を明確にすると図７のようになる。実施例では図１を利用した認証データ消去方法と図７を利用した認証データ消去方法とを利用する。携帯型情報装置１と、個人認証装置１０２と、情報伝送路１０３と、無線電話通信網７０１を利用した情報伝送路１０４とからなる。７０３は個人認証装置１０２の通信部、７０２は情報装置の通信部で無線電話接続手段やインターネット接続手段を有してもよく、実施例では無線電話網の通信に利用する。個人認証装置１０２の内部に携帯型情報装置１と同様な一定の条件を満たすと携帯型情報装置に制御データを入力するシステムを構成しておき、制御データを個人認証装置１０２の制御データ入力手段７０４により入力する。この時、使用者の特定のとき明らかにした識別番号により多数の携帯型情報装置から使用者１０１の携帯型情報装置１を特定する。携帯型情報装置１では受信した電磁波が個人認証装置１０２から送信された任意の制御データであると判定すると、条件データの条件を満たし認証データを消去する。条件データには送信予定の任意の制御データを処理する制御データ処理手順を事前に設定し付加する必要がある。情報伝送路１０３は認証データ参照手段１１２で利用し、電磁波を利用せず、接触など流出の危険性の低い安全な別の通信方法を利用する。

【００３３】図８に実施例１のフローチャートを示している。以上、図１、図２、図３、図４、図５、図６、図７を使って以下に実施例１の説明をする。

【００３４】図１はイベント会場で利用される個人認証システムである。ただし個人認証装置１０２は図３の個人認証装置３０１のように使用者特定部１０５と情報処理部１０６と認証データ参照部１０７は分離して設置され動作時にそれぞれを結ぶ情報伝送路により通信し、システム提供者が管理し所有する。使用者１０１が所有する携帯型情報装置１の画面上で使用者特定部１０５との通信によりイベントの有効期限つきの入場権利を購入し、携帯型情報装置１へ認証データＢを記憶する。さらにイベント会場で認証データ参照部１０７との通信により認証データＢを提示して個人認証して入門する。さらに、有効期限を過ぎるか、もしくは特定の制御データを受信することで、携帯型情報装置１に記憶する認証データＢを自動的に消去する。図８には個人認証準備段階と、個人認証段階と、認証データ消去段階がある。図８の使用者の特定８０１から条件データの入力８０６が個人認証準備段階で、認証データＢ参照可能８０７からサービス開始８１０は個人認証実行段階で、制御データ入力８１１からサービス利用権利失効８１４が認証データ消去段階である。

【００３５】個人認証準備段階は、サービスを受けるイベント会場の入場現場で、使用者１０１が認証データＢを記憶した携帯型情報装置１を利用して、個人認証をする準備段階である。認証データＢにより特定した使用者１０１と携帯型情報装置１を対応させるとともに、個人認証時に識別可能な認証データを発行する。さらに認証データＢを任意に消去するため条件データを入力する。使用者の特定８０１は使用者１０１を特定し、同時に個人認証システムを利用してよいかを調べる。実施例では、使用者１０１が無線電話接続手段やインターネット接続手段を有する携帯型情報装置１を操作し、システム提供者が電話番号やアドレス番号など携帯型情報装置１固有の識別番号を使用する使用者１０１から料金の徴収手段を有することを前提に、使用者１０１は識別番号の提示によりイベント会場の利用権利をシステム提供者より購入する。購入した時点で、携帯型情報装置１を操作している使用者１０１を正当な購入者する簡易的な使用者特定手段１０８である。認証データの発行８０２は、認証データＢと認証データ識別用データを同時に発行し、認証データ識別用データは個人認証装置１０２内部で記憶する。認証データの入力８０４は使用者の特定８０１で参照した固有の識別番号により特定した携帯型情報装置１へ発行した認証データＢを入力する。サービス利用権利発生８０５は、使用者１０１が認証データＢを記憶する携帯型情報装置１を所持すれば個人認証されることを示す。

【００３６】条件データの設定８０３は条件データの条件や手順を設定する。実施例では２種類の条件データＢ、Ｃを携帯型情報装置１へ入力する。システム提供者が設定した選択枠から、使用者１０１が９月８日１９時までの入場期限を選択し、９月８日１９時に時間がなると認証データＢを消去する条件データＢを設定する。条件データＢの条件は９月８日１９時を示す制御データＢが入力されることで、付加される手順は処理判定手段７の結果に従い認証データ消去手段６により認証データＢを消去する認証データ処理手順や、処理判定手段７によ

り条件データＢを処理し制御データと処理判定する条件データ処理手順や、時間情報発生部より入力される時間情報を含む制御データＢを処理判定手段７により処理する制御データ処理手順や、認証データＢを消去後条件データＢも消去する手順は条件データ処理手順に含める。実施例では条件は使用者１０１が選択するが、手順は携帯型情報装置１に備わる図５の認証データ入力手段に必要な構成や処理判定手段や認証データ消去手段を確認して個人認証装置１０２が自動的に設定する。さらに、図７のシステムを利用し、個人認証装置１０２から無線電話通信網７０１の情報伝送路を利用して制御データＣを送信し認証データを消去するために条件データＣを設定する。条件データＣの条件はシステム提供者が決めた任意の制御データＣが入力されることで、認証データ処理手順や条件データ消去手順は条件データＢと同じ内容だが、条件データ処理手順や制御データ処理手順は図５の様に制御データの種類と制御データ入力手段に必要な構成が異なるため別の内容となる。条件データ入力手段５により条件データＢと条件データＣは携帯型情報装置１へ入力され、条件データ記憶手段４で記憶する。使用者１０１は記憶済みの認証データＢを個人認証可能サービス通知手段４０４で確認し、図４の条件データ設定手段４０６により任意の条件データＤを設定してもよい。図４では認証データＢに対応していないが、認証データＢを消去する認証データ処理手順を付加して対応させる。

【００３７】個人認証実行段階は、サービスを受けるイベント入場現場で、認証データを利用して使用者１０１の個人認証をする段階である。認証データ参照部１０７に携帯型情報装置１を接触すると認証データ参照手段１１２により認証データを参照し８０７、認証データ識別手段１１１により認証データの発行８０２で発行した認証データ識別用データと認証データＢを処理し認証データの識別８０８をすることで使用者の個人認証８０９をする。個人認証をすると、使用者１０１はサービス利用許可手段１１３により門が開き入門を許されサービスの開始８１０となる。

【００３８】認証データ消去段階は、サービスを受けた後、使用者１０１やシステム提供者にとって、不要となった認証データＢを消去する段階である。サービスを受けないで消去するケースもある。制御データの入力８１１は制御データ入力手段８もしくは制御データ入力手段７０４により制御データを入力する。条件データと認証データは処理判定手段７により処理され条件データの条件を満たすか判定８１２され、条件を満たすと認証データの消去８１３となる。条件データＢと条件データＣにより別に認証データ消去方法を説明する。条件データＢを利用した認証データＢの消去は図１の構成を利用する。携帯型情報装置１には時間情報発生部より制御データＢを入力しており、処理判定手段７において認証データ処理手順に従って制御データＢは処理され、条件データ処理手順に従って条件データＢは処理されている。制御データＢに任意の時刻を示すデータを含むことで条件データＢの条件を満たす判定がなされると、認証データ処理手順に従い認証データ消去手段６により認証データＢを消去する。条件データＣを利用した認証データＢの消去は図７の構成を利用する。システム提供者の任意な時に情報伝送路１０４を利用して個人認証装置１０２から携帯型情報装置１へ制御データＣを入力する。処理判定手段７において認証データ処理手順に従って制御データＣは処理され、条件データ処理手順に従って条件データＢは処理される。制御データＢに任意のデータを含み条件データＣの条件を満たす判定がなされると、認証データ処理手順に従い認証データ消去手段６により認証データＢを消去する。認証データＢの消去により、個人認証できなくなりサービス利用権利失効８１４する。また、図６の構成を利用して利用回数により自動的に認証データＢを消去するようにしてもよい。システム提供者や使用者１０１が設定した有効期限を過ぎたり、任意の制御データを無線電話網により受信することで認証データＢを携帯型情報装置１から自動的に消去することで、盗難による不必要な認証データの流出を未然に防止し、管理の煩わしさを軽減し、さらに、情報装置の記憶容量を有効に活用することが可能となる。

【００３９】（実施例２）自宅の玄関の開鍵に使用する自宅セキュリティシステムの個人認証システムと、会社の玄関の開鍵に使用する社内セキュリティシステムの個人認証システムとからなる。図１と図３は、実施例２の個人認証システム構成図である。図１、図２、図３、図４、図５を使って以下に実施例２の説明をする。２つの認証データをそれぞれの個人認証システムで独立して使用する。会社セキュリティシステムで利用する認証データＡは社内で利用後に会社出口にて自動的に消去され記憶容量の確保がなされるとともに、使用者が認証データ管理に煩わされることもない。自宅セキュリティシステムで利用する認証データＢは携帯型情報装置１の破壊感知や、謝ったパスワードの入力により消去され、盗難による認証データの流出や不正利用を防止する。

【００４０】会社セキュリティシステムの個人認証システムは、図３のシステム構成を利用する。個人認証装置３０１は、使用者特定部３０４と、情報処理部３０５と、認証データ参照部３０６とに分離して設置してあり、認証データＡを使用する。自宅セキュリティシステムの個人認証システムは、図１のシステム構成を利用し、認証データＢを使用する。実施例１と異なるのは個人認証装置１０２と、個人認証装置３０１がそれぞれ違う装置であり、２つの独立した個人認証システムで使用者１０１が所持する１台の携帯型情報装置１を利用して個人認証する点である。

【００４１】会社セキュリティシステムの個人認証システムのシステム構成を図３に基づいて説明する。使用者

携帯の携帯型情報装置１と、会社に設置されている個人認証装置３０１とからなる。個人認証装置３０１は、門前に設置された使用者特定部３０４と、会社内部各ドアに設置された複数の認証データ参照部３０６と、発行した認証データを識別する情報処理部３０３とからなる。使用者特定部３０４と情報処理部３０５、さらに認証データ参照部３０６と情報処理部３０５はそれぞれ有線の情報伝送路３０２、３０３で接続してある。携帯型情報装置１と使用者特定部３０４と、携帯型情報装置１と使用者参照部３０６はともに接触による同じ通信方法を採用した情報伝送路３０７、３０８を有する。使用者特定部３０４は少なくとも使用者特定手段３０４と、認証データ入力手段３０９を有し、その他に条件データ入力手段３１０を有する。情報処理部３０５は少なくとも認証データ識別手段３１２を有し、同時に認証データＡを発行し認証データ識別用データを使用者の個人情報などと共にデータベースなどを利用して一元管理し記憶してよい。認証データ参照部３０６は、少なくとも認証データ参照手段３１３を有し、認証データ識別手段３１２により認証データＡを識別するとドアが開く。さらに、複数の認証データ参照部３０６の内、会社出口のドアに設置する認証データ参照部３０６のみが制御データ入力手段３１４を有す。

【００４２】利用方法について説明する。使用者１０１は携帯型情報装置１０１を会社の門前に設置してある使用者特定部３０４へ接触させ、さらに指紋などバイオメトリにより使用者特定手段３１１により特定される。情報処理部３０５に記憶する過去に測定した社員の生体情報と一致すると、使用者特定部３０４に接触している携帯型情報装置１へ後で識別可能な認証データＡを認証データ入力手段３０９により入力する。携帯型情報装置１は認証データＡを認証データ記憶手段４で記憶する。同時に、使用者参照部３０６との通信により制御データＡを入力されることを条件とし、処理判定手段７と認証データ消去手段６を利用して認証データＡを消去する認証データ処理手順や、制御データＡを処理する制御データ処理手順や、条件データＡと制御データＡを処理する条件データ処理手順を付加し条件データＡとして自動的に設定し、条件データ入力手段３１０により携帯型情報装置１へ入力する。携帯型情報装置１は条件データＡを条件データ記憶手段４で記憶する。使用者１０１は会社内で携帯型情報装置１を認証データ参照部３０６に接触することで、個人認証され、ドアが開くことで通過する。退社時に、出口の門に設置した認証データ参照部３０６に接触すると、制御データ入力手段３１４により制御データＡが入力される。制御データＡは条件データＡと処理判定手段７により処理され、条件データＡの制御データＡを入力される条件を満たすことで、認証データ消去手段６により携帯型情報装置１に記憶する認証データＡを消去する。この前後、出口ドアが開き、使用者１０１は認証データＡが消去された携帯型情報装置１を所持して自宅へ向かう。会社用の認証データＡは毎日変更し、更新するため、安全性を向上することが可能になる。

【００４３】自宅セキュリティシステムの個人認証システムの構成について図１に基づいて説明する。使用者携帯の携帯型情報装置１と、自宅に設置する個人認証装置１０２と、接触による同じ通信方法を採用した情報伝送路１０３、１０４とからなる。個人認証装置１０２は家のドアに設置する。個人認証装置１０２内の使用者特定部１０３は使用者特定手段１０８と、認証データ入力手段３と、条件データ設定手段１０９と、条件データ入力手段５とを有する。情報処理部１０６は認証データ発行手段１１０と認証データ識別手段１１１とを有する。使用者特定部１０５と情報処理部１０６は家の内側に設置され、家の外からは操作できない。条件データ設定手段１０９や、条件データ入力手段５や、認証データ発行手段１１０は使用者特定部１０５、もしくは情報処理部１０６のどちらにあってもよい。認証データ参照部１０７は認証データ参照手段１１２と、サービス利用許可手段１１３を有する。認証データ参照部１０７はドアの外側に設置され、家の外で携帯型情報装置１内の認証データを参照し、識別することでドアを開く。

【００４４】利用方法について説明する。使用者１０１は外出前、使用者特定部１０５に携帯型情報装置１を接触する。個人認証装置１０２は記憶する識別番号に一致すると、携帯型情報装置１へ認証データＢを入力する。同時に、携帯型情報装置１の制御データ入力手段８を確認して破壊衝撃を感知することを条件とする条件データＢを条件データ設定手段１０９が自動的に設定し条件データ入力手段５により入力する。条件データＢは携帯型情報装置１の有する衝撃センサーの信号を制御データとして処理する制御データ処理手順や、条件データ処理手順や、認証データ処理手順を含むプログラムも同時に付加される。さらに、使用者１０１は条件データ設定手段４０６によりパスワード以外のデータを携帯型情報装置１へ入力することを条件とする条件データＣを設定し、条件データ入力手段４０２により入力する。条件データＣは携帯型情報装置１の有する入力部からの入力を制御データとして処理する制御データ処理手順や、条件データ処理手順や、認証データ処理手順を含むプログラムも同時に付加される。条件データＢと、条件データＣは条件データ記憶手段４に記憶する。図２に示すとおり認証データＢは条件データＢ、もしくは条件データＣをみたすと消去される。会社内では認証データＡと条件データＡも記憶して複数の認証データと条件データが携帯型情報装置１に存在する。帰宅後、携帯型情報装置１をドア外側の認証データ参照部１０７に接触し、通信開始を指示するパスワードを携帯型情報装置１へ入力すると、個人認証装置１０２は認証データＢを参照し、認証データＢを認証データ識別手段１１１で識別するとサービス利

用許可手段１１３によりドアが開く。帰宅途中、携帯型情報装置１の盗難に遭い、記憶素子を取り出すなど破壊衝撃をセンサーが感知した信号が制御データとして入力されると、処理判定手段７により条件データＢと処理し、破壊衝撃を感知するという条件データＢの条件を満たす判定により、認証データ消去手段４により認証データＢを消去する。また、他人が誤ったパスワードを制御データとして入力すると、処理判定手段７により条件データＣと処理し、パスワード以外のデータをを入力するという条件を満たすとの判定により、認証データ消去手段４により認証データＢを消去する。

【００４５】携帯型情報装置１の詳細を図４について説明する。認証データ記憶手段２と、条件データ記憶手段４と、認証データ消去手段６と、条件データと制御データを処理し判定する処理判定手段７と、制御データ入力手段８とを有す。さらに個人認証装置３０１から制御データ入力手段３１４により制御データを入力されるまた、自宅のセキュリティに使用する、識別番号記憶手段４０７と、制御データ入力手段８として入力ボタンと衝撃を感知する圧力センサもしくは、変位センサを有する。図５に示す他の制御データ入力手段を有するなら、ある電磁波を受け取ったり、ある時間になったり、使用者１０１の生体情報が測定できなくなったり、ある地域より外へ出たりすることで認証データを消去することが可能となる。その他に、図４で示すように、携帯型情報装置１は内部に条件データ設定手段４０６と条件データ入力手段４０２を有し記憶している認証データから任意の認証データを特定して消去するよう条件データを、その外に、携帯型情報装置１は認証データ消去条件通知手段４０３や、個人認証可能サービス通知手段４０４や、認証データ消去予告手段４０５などを有してよい。これら手段を携帯型情報装置１が有することで使用者１０１の利便性は向上する。このように、認証データＡや、認証データＢを携帯型情報装置１から個別に消去することで、利用分野の多様化に適応し、盗難による不必要な認証データの流出を未然に防止し、管理の煩わしさを軽減し、さらに、情報装置の記憶容量を有効に活用することが可能となる。

【００４６】（実施例３）本例は高額の商品購入に使用する個人認証システムである。図１、図２、図４、図５、図６に基づいて説明する。

【００４７】図１によりシステムの構成を説明する。本実施例の個人認証システムは使用者１０１が携帯の携帯型情報装置１と、個人認証装置１０２とからなる。個人認証装置１０２は、電子商取引をする複数の個人宅のコンピュータに内蔵された使用者特定部１０５と、複数の小売店に設置される認証データ参照部１０７と、システム提供者である銀行やカード会社などにおかれた１つ以上の情報処理部１０６からなり、図３の個人認証装置３０１と同様に分離されているが有線の情報伝送路にて接続され、動作時は一つの装置として機能する。携帯型情報装置１と使用者特定部１０５間には赤外線を利用した無線の情報伝送路１０４、携帯型情報装置１と認証データ参照部１０７には接続することでデータの送受信する有線の情報伝送路１０３を有する。個人認証装置１０２に属する使用者特定部１０５は使用者特定手段１０８と、認証データ入力手段３と、条件データ設定手段１０９と、条件データ入力手段５とを有し、使用者１０１の特定後に発行した認証データと設定した条件データを携帯型情報装置１へ入力する。認証データ参照部１０７は、認証データ参照手段１１２と、サービス利用許可手段１１３とを有し、携帯型情報装置１と接触すると情報伝送路１０３により認証データＡを参照する。情報処理部１０６は認証データ発行手段１１０と認証データ識別手段１１１とを有し、データベースなどを利用して個人情報や、認証データ識別データや、個人認証システムの利用状況などを一元管理するとともに、認証データ識別手段１１１を効率的に管理可能となる。認証データ発行手段１１２によりシステム提供者は認証データの発行も手元で管理し、常に最新の暗号技術による認証データを利用する。

【００４８】携帯型情報装置１は認証データ記憶手段２と、条件データ記憶手段４と、認証データ消去手段６と、処理判定手段７と、制御データ入力手段８とを有す。また、制御データ入力手段８として制御データを入力するため、生体情報を測定する生体情報サンプリング部と、位置情報を測定する位置情報取得部とを有し、図６に示すように処理判定手段７には条件データ変更手段６０１を有す。図５に示す制御データ種類による構成を有し、任意の電磁波を受け取ったり、任意の日時になったり、任意のパスワード以外の入力したり、任意の破壊による衝撃を感知することで任意に認証データを消去してもよい。さらに、図４で示すように携帯型情報装置１は内部に条件データ設定手段４０６や、条件データ入力手段４０２や、認証データ消去条件通知手段４０３や、個人認証可能サービス通知手段４０４や、認証データ消去予告手段４０５などを有してよい。これら手段を有することで、携帯型情報装置１による個人認証システムの利用を利便性よくし、効率性は向上する。

【００４９】利用方法について説明する。使用者１０１は自宅で電子商取引用コンピュータにＩＣカードを差込み、携帯型情報装置１と使用者特定部１０５間で情報伝送路１０４により通信を開始する。バイオメトリによりＩＣカードに記憶する生体情報と一致すると、使用者１０１を使用者特定手段１０８により特定する。同時に使用者特定部１０５と通信している携帯型情報装置１へ認証データ発行手段１１０により発行した認証データＢを情報伝送路１０４を利用して入力する。認証データＢは携帯型情報装置１の認証データ記憶手段２に記憶する。ＩＣカードは唯一無二の生体情報を記憶しているので外

出時には持ち歩かない。さらに条件データ設定手段１０９により、生体情報測定値を含む制御データＢに一定変化を生じると認証データＢを消去する条件データＢと、電子商取引用コンピュータで選択した購入予定の小売店の位置情報以外の位置情報を含む制御データＣの入力により認証データＢを消去する条件データＣとを設定する。条件データ入力手段５により条件データＢと条件データＣは情報伝送路１０４を利用して携帯型情報装置１へ入力し、条件データ記憶手段４に記憶する。使用者１０１は個人認証サービス通知手段４０４で目的の認証データＢを携帯型情報装置１に記憶したことを確認すると、携帯型情報装置１内の条件データ設定手段４０６により使用限界の金額を条件データＤの条件として設定する。条件データＤは条件データ記憶手段５で記憶される。条件データＤは条件データ変更手段６０１を有する携帯型情報装置１に出荷時に何種類か設定されていて携帯型情報装置１を利用した１つの認証データでの最大取引金額を制限し安全性を高めている。図２のように条件データＤは認証データＢに対応していないが、条件データ設定手段４０６により認証データＢを消去する認証データ処理手順を付加して認証データＢを消去するための条件データＤとなる。このように複数の条件データが１つの認証データに対応して記憶されている。

【００５０】小売店のレジにおいて、携帯型情報装置１を使用者参照部１０５に接触すると、認証データ参照手段１１２により認証データ記憶手段２と通信を開始し、認証データ識別手段１１１により認証データＢを認証データ識別用データと処理し識別する。認証データＢを識別するとサービス利用許可手段１１３として使用者１０１が本人であることの表示が使用者参照部１０５のパネル上に表示され、店員は商品を使用者１０１へ渡す。さらに使用者１０１の銀行口座より決算される。決算は認証データを携帯型情報装置１へ入力するときになされてもよい。制御データ入力手段８により入力される使用者１０１の生体情報を含む制御データＢは処理判定手段７により条件データＢと処理さる。外出中に携帯型情報装置１の盗難に遭い使用者１０１の手元から離れると、制御データＢに変化を生じ、例えば制御データＢが一定の電圧値より下回ると条件データＢの条件を満たすことで条件データＢに付加されている認証データ処理手順に従って動作される認証データ消去手段６により携帯型情報装置１内部で認証データＢを消去する。制御データＢは制御データ処理手順に従って、条件データＢは条件データ処理手順に従って処理判定手段７により処理する。また、他人が購入予定外の小売店の個人認証装置と通信すると、設定以外の小売店の位置情報が制御データＣとして入力され条件データＣを満たすことで認証データＢを消去する。その他に購入ごとに、使用した金額が制御データＤとして携帯型情報装置１に入力され、図６の条件データ変更手段６０１により、条件データＤの条件である使用限界金額から引かれ、０に近くなると、条件データＤを満たすことで、認証データ消去手段４により認証データＢを消去する。このように各種の条件データを事前に設定し携帯型情報装置１に記憶することで、認証データＢを携帯型情報装置１から消去して盗難による不必要な認証データの流出を未然に防止し、管理の煩わしさを軽減し、さらに、携帯型情報装置の記憶容量を有効に活用することが可能となる。

【００５１】

【発明の効果】本発明によれば、携帯型情報装置に記憶する認証データを任意に消去する。したがって、不必要な認証データの流出や、携帯型情報装置の記憶容量の不足などを防ぎ、使用者やシステム提供者が個々に安全性、効率性を向上できる。

【００５２】さらに、本発明によれば、携帯型情報装置に記憶する特定の認証データを任意に消去する。したがって、携帯型情報装置に複数で記憶される認証データの制御性を向上し、個人認証システムの多様化に対応する。

【００５３】さらに、本発明によれば、携帯型情報装置に記憶する特定の認証データを自動に消去する。したがって、携帯型情報装置の管理で使用者が、複数の認証データの管理をする煩わしさがなくなり、個人認証システムの効率性を向上する。

【図面の簡単な説明】

【図１】本発明の携帯型情報装置とこれを含んだ個人認証システムの構成図である。

【図２】本発明における認証データと条件データの対応である。

【図３】本発明の携帯型情報装置とこれを含んだ個人認証システムの構成図である。

【図４】本発明の携帯型情報装置とこれを含んだ個人認証システムの構成図である。

【図５】本発明の制御データ種類と制御データ入力手段に必要な構成の関係を示した図である。

【図６】本発明の携帯型情報装置とこれを含んだ個人認証システムの構成図である。

【図７】本発明の携帯型情報装置とこれを含んだ個人認証システムの構成図である。

【図８】本発明の携帯型情報装置における認証データ消去方法を示すフローチャートである。

【符号の説明】

１　携帯型情報装置
２　認証データ記憶手段
３　認証データ入力手段
４　条件データ記憶手段
５　条件データ入力手段
６　認証データ消去手段
７　処理判定手段
８　制御データ入力手段

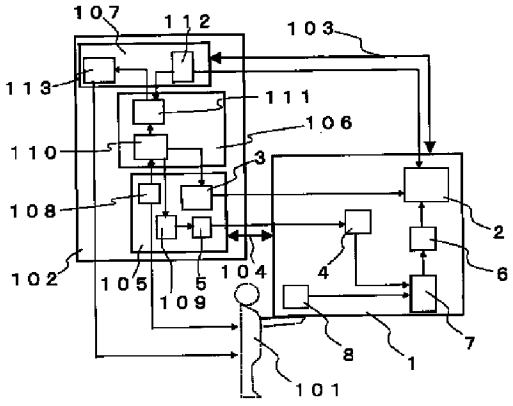
25

１０１　使用者
１０２　個人認証装置
１０３　情報伝送路
１０４　情報伝送路
１０５　使用者特定部
１０６　情報処理部
１０７　認証データ参照部
１０８　使用者特定手段
１０９　条件データ設定手段
１１０　認証データ発行手段
１１１　認証データ識別手段
１１２　認証データ参照手段
１１３　サービス利用許可手段
２０１　認証データＡ消去用条件データＡ
２０２　認証データＢ消去用条件データＢ
２０３　認証データＢ及びＣ消去用条件データＣ
２０４　条件データＤ
２０５　認証データＤ
３０１　個人認証装置
３０２　情報伝送路
３０３　情報伝送路
３０４　使用者特定部
３０５　情報処理部
３０６　認証データ参照部
３０７　情報伝送路

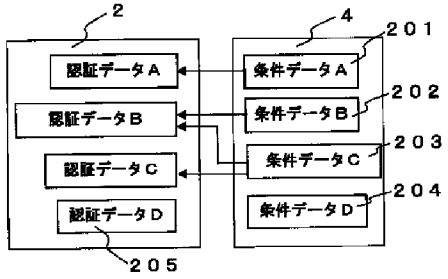
26

＊３０８　情報伝送路
３０９　認証データ入力手段
３１０　条件データ入力手段
３１１　使用者特定手段
３１２　認証データ識別手段
３１３　認証データ参照手段
３１４　制御データ入力手段
４０１　情報伝送路
４０２　条件データ入力手段
４０３　認証データ消去条件通知手段
４０４　個人認証可能サービス通知手段
４０５　認証データ消去予告手段
４０６　条件データ設定手段
４０７　識別番号記憶手段
６０１　条件データ変更手段
７０１　個人認証装置
７０２　無線電話通信網
７０３　情報伝送路
７０４　通信部
７０５　認証データ入力手段
７０６　条件データ入力手段
７０７　制御データ入力手段
７０８　通信部
７０９　認証データ参照手段
＊

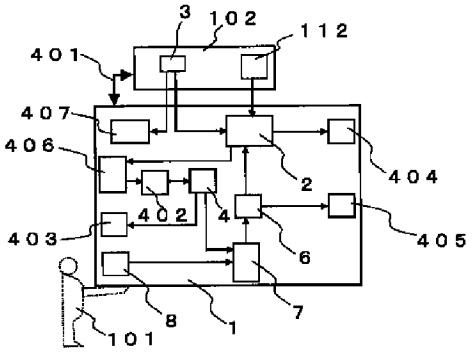
【図１】



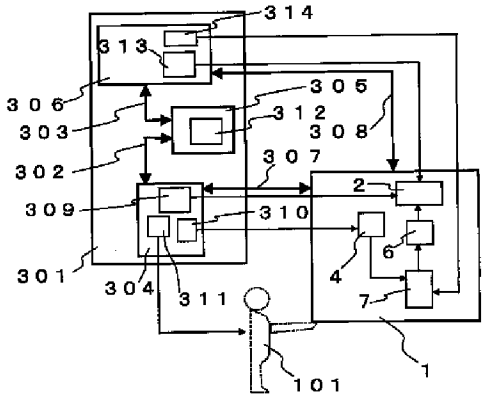
【図２】



【図４】



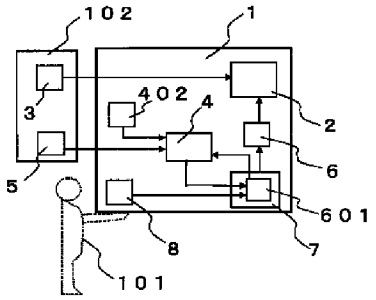
【図３】



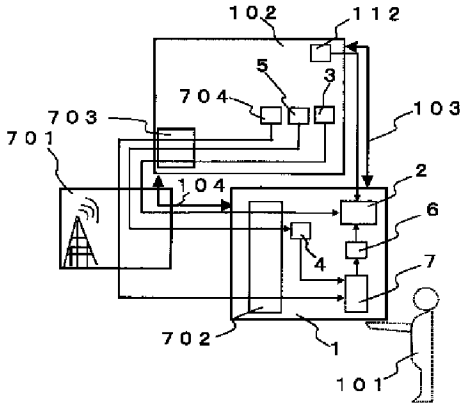
【図５】

制御データ種類	制御データ入力手段に必要な構成
外部から受信した電磁波から得る制御データ	通信部
入力部から入力する制御データ	入力部
時間情報より得る制御データ	時間情報発生部，もしくは時間情報受信部
使用者の生体情報より得る制御データ	生体情報サンプリング部
位置情報より得る制御データ	位置情報取得部
信号情報より得る制御データ	信号発生部

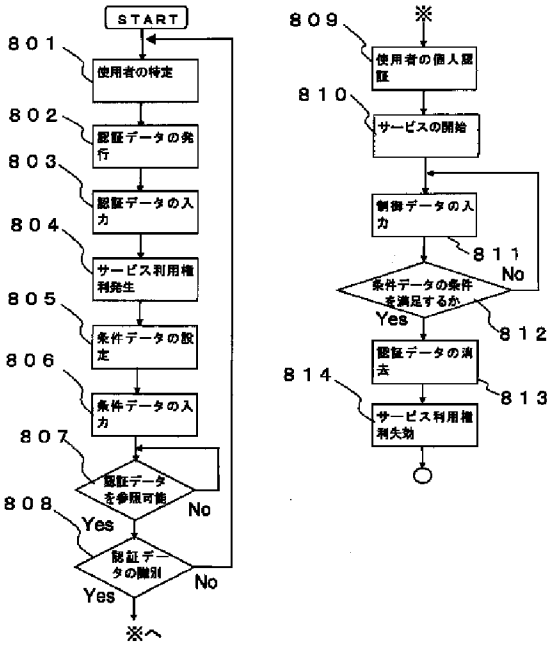
【図６】



【図７】



【図８】


START
801
使用者の特定
802
認証データの発行
803
認証データの入力
804
サービス利用権利発生
805
条件データの設定
806
条件データの入力
807
認証データを参照可能
No
808
Yes
認証データの識別
No
Yes
※へ
809
※
使用者の個人認証
810
サービスの開始
制御データの入力
811
No
条件データの条件を満足するか
Yes
812
認証データの消去
813
814
サービス利用権利失効